C.1 BACKGROUND

The Marine Corps Network Operations and Security Center (MCNOSC) is the Marine Corps' nucleus for enterprise data network services, network support to deploying forces, and technical development of network-enabled Information Technology (IT) solutions. The MCNOSC is responsible for the operation and defense of the Marine Corps Enterprise Network (MCEN) and its hosted information systems and services. The MCNOSC is also responsible for Command and Control (C2) capabilities for Fleet Marine Forces and garrison forces stationed around the world. The MCNOSC is also responsible, at an enterprise level, for the defense and protection of the MCEN and providing associated technical leadership and management support of enterprise services and devices. The MCNOSC provides support of the MCEN and Fleet Marine Forces from a primary site in Quantico, VA, and a secondary site in Kansas City, MO as indicated for each task throughout this PWS. Eight Marine Air-Ground Task Force (MAGTF) Information Technology (IT) Support Centers (MITSCs) are responsible for the management and compliance of devices (specifically workstations and other endpoints) within their regions. From inside the MCNOSC Quantico Operations Center, personnel monitor network operations 24x7x365 (not solely Federal business days) through an array of strategically positioned sensors to ensure the availability and security of the MECN. The Operations Center monitors three major areas of the MCEN: (1) threats and vulnerabilities, (2) Information Technology (IT) systems status, and (3) performance and Joint and USMC deployed operations.

The Marine Corps Enterprise Network (MCEN) is comprised of two components, the unclassified NIPRNET (MCEN-N) and the classified SIPRNET (MCEN-S). There are currently approximately 76,000 managed assets on the MCEN-N, and 8,000 on the MCEN-S. The MCEN provides the Marine Corps with connectivity to defend network and mainframe services essential for accomplishing everyday tasks. The MCEN enables business, warfighting and command and control (C2) capabilities from the Supporting Establishment in garrison and forward deployed Operating Forces to the Joint Information Environment and Department of Defense Information Network. The MCEN encompasses the entirety of the USMC's general service Non-secure Internet Protocol Router Network (NIPRNET) and classified Secret Internet Protocol Router Network (SIPRNET) common user network environments, including all communication circuits and attached devices and systems. The MCEN is comprised of the garrison network (both NMCI and Legacy), deployed/tactical networks, and infrastructure that supports access to Defense Information Systems Agency (DISA) managed mainframe computer services. The MCEN is the Marine Corps' portion of the overall DoD Global Information Grid (GIG) and is a designated National Security System (NSS). The NIPRNET, which transverses the MCEN Points of Presence (POPs) on the Wide Area Network (WAN), is a DISA-facilitated DoD NSS.

The MCEN is comprised of over 200,000 users positioned behind NIPRNET and SIPRNET tier 2 and 3 boundaries at over 30 bases/posts/stations and a varying number of deployed locations around the globe. Each tier 2 and 3 boundary is under MCNOSC oversight and consists of an integrated suite of firewalls, routers, switches, and virtual private network devices. Behind these boundaries are MCNOSC managed enterprise virtual server infrastructure, storage area networks and messaging environment. In all, the MCNOSC manages over 5,000 physical and virtual systems on the MCEN world-wide.

The objective of this PWS is to support the MCNOSC in carrying out the technical, engineering, operations, maintenance, and management functions that support global network operations and defense of the Marine Corps Enterprise Network (MCEN). The Contractor support will enable the MCNOSC to maintain a tightly integrated, agile, defensible, survivable network capable of supporting highly distributed operations as well as an efficient and effective business enterprise.

C.2 SCOPE

The scope of this PWS includes support services for the monitoring and operation of the MCEN to ensure the availability and security of the network and to remain responsive to the demands of the MCEN. The contractor shall perform work at the designated sites specified throughout the PWS. Not all tasking requires 24x7x365 support and level of support is defined in each PWS section.

The scope of tasking includes the following tasks which will be detailed in section C.4:

Task C.4.1: Program Management
- Subtask C.4.1.1: Coordinate a Project Kickoff Meeting
- Subtask C.4.1.2: Prepare a Monthly Status Report
- Subtask C.4.1.3: Meeting Minutes
- Subtask C.4.1.4: Convene Technical Status Meetings
- Subtask C.4.1.5: Prepare a Project Management Plan
- Subtask C.4.1.6: Update the Project Management Plan
- Subtask C.4.1.7: Prepare Trip Reports
- Subtask C.4.1.8 Transition-In/Implement Transition-In Plan
- Subtask C.4.1.9: Transition Out/Implement Transition-Out Plan

Task C.4.2: Cyber Support Branch Technical Services (Operations Division)
- Subtask C.4.2.1: Network Common Operational Picture (NETCOP) Support
- Subtask C.4.2.2: Assured Compliance Assessment Solution (ACSS) Support

Task C.4.3: MCEN Operations Support (Operations Division)
- Subtask C.4.3.1: Operations Center Support
- Subtask C.4.3.2: Enterprise Directory and Messaging (EDM) Support
- Subtask C.4.3.3: Integrated Network Support (INS)

Task C.4.4: Local IT Communications Support (Support Division)
- Subtask C.4.5.1: Local IT, Information Assurance, and Network Support

Task C.4.5: Project Implementation Support (Operations Division)

C.3 APPLICABLE DOCUMENTS

Unless otherwise supplemented or superseded, Directives applicable to the performance of the subject work are as follows:

- Information Technology Infrastructure Library (ITIL) version 3 framework established guidelines for the Information Technology Service Management (ITSM) discipline for managing information technology (IT) systems.
- Department of Defense Directive 8570-1 (DoDD 8570-1) - Information Assurance. Training, Certification, and Workforce Management. 12-2005 with Incorporated change of 4-20-2010.
- MARINE CORPS ORDER (MCO) 5510.18A- United States Marine Corps Information and Personnel Security Program Manual
- Secretary of the Navy-SECNAVINST 5510.30B- Department of the Navy (DON) Personnel Security Program (PSP) Instruction
- Secretary of the Navy (SECNAV M-5510.30)--Department of the Navy Personnel Security Program
- Secretary of the Navy (SECNAVINST) 5510.36A- Department of the Navy (DON) Information Security Program (ISP) Instruction
- Secretary of Navy (SECNAV) M-5510.36-Department of the Navy Information Security Program Manual, 1 Jul 06
- Marine Corps Base Order (MCBO) 5510.1C- Information and Personnel Security Program (IPSP)
- Marine Administrative Message (MARADMINS) and United States Marine Corps (USMC) Operational Directives as tasked
- Marine Corps Cyber Operations Group (MCCOG) policies, procedures and Standard Operating Procedures (SOP) (Available Upon Award)
- Additional Regulatory Guidance: As needed per specific tasking, the Contractor shall apply Marine Corps, Department of the Navy and the Department of Defense Information Assurance policies, procedures, and technical communication requirements as defined under the following, which can be found through the Defense Information Systems Agency (DISA) portal at iase.disa.mil, and United States Cyber Command, https://www.cybercom.mil/default.aspx, under the orders and Directives tab. For example, Risk Management Framework Security Technical Information Guides required for certification and accreditation activities under Task C.5.4.

All products, processes, and procedures must adhere to government provided standards to include local SOPs, DISA, DoD, USMC, and other government directives and guidelines.

C.4 TASKS

C.4.1 PROGRAM MANAGEMENT

All subtasks under this section are required to be performed during normal business hours (8 hrs x 5 days/week x 52 weeks (8x5x52) (Federal business days) at Quantico, VA location.
The The Contractor shall provide program management support. Tasking includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The Contractor shall identify a Program Manager (PM) by name who shall provide management, direction, administration, quality assurance, and leadership of the execution of tasking. The PM shall serve as the Government's primary point-of-contact and provide technical supervision and guidance for all contractor personnel assigned to support the MCNOSC.

Performance Standards and Acceptable Quality Level for Task 1: See attached Performance Requirement Summary (PRS) below.

C.4.1.1 COORDINATE A PROJECT KICK-OFF MEETING

The Contractor shall schedule and coordinate a Project Kick-Off Meeting (CDRL A001) to occur within three business days of contract award at a location hosted by the government, located at Quantico, VA. The meeting will serve as an introduction between the contractor personnel and Government personnel who will be involved with tasking. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include the Government Technical Point of Contact (TPOC), contractor personnel able to answer questions and conduct the kickoff meeting, the Contracting Officer's Representative (COR) and other relevant Government personnel. The Contractor shall provide a status of transition Activities (e.g. Clearances, Communication/Organizational Awareness, Personnel), Government actions required, and a plan for the contractor to deploy resources to keep the network operational.

C.4.1.2 PREPARE A MONTHLY STATUS REPORT (MSR)

The Contractor PM shall develop and provide a MSR (CDRL A007) using Microsoft (MS) Office Suite applications, by the tenth of each month via electronic mail to the Technical Point of Contact (TPOC) and the COR.

The MSR shall include the following:

- Activities during reporting period, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- Personnel gains, losses, and status (security clearance, etc.).
- Government actions required.
- Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for the reporting period).

C.4.1.3 MEETING MINUTES

The Contractor shall prepare and deliver Meeting and Review Minutes (CDRL A008) for all meetings specified in this PWS or else identified by the Government Notes shall be provided to the Government within 24 hours of meeting and Government acceptance shall occur with 48 hours thereafter. At a minimum the minutes shall contain the following: Date and place, Attendees, Purpose of meeting/review, Brief description of items discussed, Results/Outcome, and Action items.

C.4.1.4 CONVENE TECHNICAL STATUS MEETINGS

The Contractor PM shall convene a monthly Technical Status Meeting (CDRL A005) with the TPOC, COR, Contractor technical Subject Matter Experts as necessary, and other Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish

priorities, and coordinate resolution of identified problems or opportunities. The Contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five workdays following the meeting.

C.4.1.5 PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The Contractor shall document all support requirements in a PMP. The PMP shall:

a. Describe the proposed management approach for all tasks in the PWS.
b. Contain detailed Standard Operating Procedures (SOPs) for all tasks.
c. Include milestones, tasks, and subtasks required in this PWS.
d. Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations.

The Contractor shall provide the Government with a draft PMP on which the Government will make comments. The final PMP (CDRL A006) shall incorporate the Government's comments. See section C.5.5 for the SSCPAC Project Management Plan Review Checklist.

C.4.1.6 UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The PMP shall be updated annually at a minimum. The Contractor shall work from the latest Government-approved version of the PMP (CDRL A006).

C.4.1.7 PREPARE TRIP REPORTS

Trip Reports are required for all travel (CDRLA009). The Contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, the cost of travel, and point of contact (POC) at travel location.

C.4.1.8 TRANSITION-IN PLANNING AND EXECUTION

The Contractor shall propose a draft Transition-In Plan as a part of their submitted proposal (see submission requirements, Section L of Request for Task Order Proposal (RFTOP)). The final Transition Plan (CDRL A004) shall be submitted at the Project Kick-Off Meeting in combination with reporting on progress of transition activities. The Contractor shall implement its Transition-In Plan immediately upon award. The Transition-In Plan shall address how the contractor will ensure continuity of service while meeting specified performance standards. At a minimum, the Transition-In Plan shall address the following areashe contractor's overall approach to ensuring a seamless transition in services, ensuring no disruption of service. NOTE: the most critical services that cannot experience a gap during transition are the operations support division services outlined in PWS Section C.4.3. These services should be prioritized for the purpose of developing and implementing the Transition-In Plan. The services in the PWS, in order of priority for continuity of service, are as follows: C.4.3, C.4.2, C.4.4, C.4.1, and C.4.5. A minimum 50% of the contract staff with adjudicated security clearances and 8570 certified shall be immediately available for tasks C.4.3 & C4.2 to facilitate onboarding processing. Without an adjudicated security clearance and 8570 certification, no administrative permissions can be given to an individual regardless of their skill sets or whether they are a contractor, government civilian or Marine.

The Transition Plan shall include at a minimum:

a. Project management processes that the contractor will use to manage the transition effort.

b. The contractor's transition management team capable of providing overall management and logistical support of all transition activities.
c. How the contractor will handle transition of Key Personnel, including obtaining required security clearances and abbreviated resumes summarizing qualifications of Key Personnel (See PWS Section C.8.3 for description of key personnel).
d. How the contractor will provide the level of cleared staffing required to perform under this contract.
e. How the contractor will obtain required Top Secret facility clearance and Special Security Office (SSO) approvals prior to commencing work.
f. Schedules and milestones, including a resource-loaded project management schedule. Milestones and measurable commitments shall be included in the schedule. The activities performed during the transition shall begin on the effective date of the Contract.

C.4.1.9 TRANSITION OUT PLANNING AND EXECUTION

The Transition-Out Plan shall facilitate the transition without disruption in service from the incumbent to an incoming Contractor or to Government personnel at the expiration period of performance. The Contractor shall provide a draft Transition-Out Plan (CDRL A003) NLT 90 calendar days prior to expiration of the period of performance. The final plan is due 45 days prior to the end of the period of performance. All information pertinent to implementing this plan shall be delivered to the government NLT 30 days prior to end of period of performance. The Contractor shall identify a plan for coordination with the incoming Contractor and/or Government personnel and describe plans for knowledge transfer for the following:

a. Project management processes
b. Points of contact
c. Location of technical and project management documentation
d. Status of ongoing technical initiatives
e. Plan for contractor to contractor coordination
f. Transition of Key Personnel
g. Schedules and milestones for transition activities and high priority activities determined by the MCNOSC
h. Disclosure of any actions that may be required of the Government to facilitate transition

The Contractor shall also establish and maintain communication with the incoming Contractor/Government personnel for the period of the transition meaning that they will transfer knowledge, passwords, and documents necessary to facilitate the transition and prevent a gap in service.

C.4.2 CYBER SUPPORT BRANCH TECHNICAL SERVICES (OPERATIONS).

For all subtasks under C.4.2, refer to section C.5. Additional Supporting Information for required response times and performance metrics.

Performance Standards and Acceptable Quality Level for Task C.4.2: See attached PRS below.

C.4.2.1 NETWORK COMMON OPERATIONAL PICTURE (NETCOP) SUPPORT

The mission of NetCOP is to develop, operate, and maintain enterprise tools and systems to provide situational awareness of network health, vulnerabilities, threats, and events within the MCEN and to operate and enhance enterprise tools enabling IT service support and operational management. NetCOP Support includes comprehensive Operations and Maintenance (O&M) of USMC enterprise and information systems, both unclassified and classified, deployed in support of the NetCOP mission. The current systems employed by NetCOP are:

NetCOP System	Supporting Technology
Enterprise Remedy IT Service Management Suite (ERIS)	Based on BMC ITSM Suite (Remedy)
	BMC Analytics and Business Objects Reporting technologies
	Apache Tomcat Web Server
	Oracle Relational Database technologies
MCEN Event Management System (MEMS)	Based on HP Enterprise Management Software (OpenView) technologies
	Microsoft IIS and Apache Tomcat Web Servers
	Oracle and SQL Server Relational Database technologies
Operational Directives Reporting System (OPDRS)	Based on custom ASP.net C# web development technologies
	SQL Server Relational Database technologies
Custom NetCOP Tools and Displays	Based on custom SharePoint and JavaScript technologies
	SQL Server Relational Database technologies
NETSCOUT	NETSCOUT nGenius Service Assurance
	Apache Tomcat Web Server

The contractor shall provide 24x5x52 (Federal business days) on site NetCOP support from the MCNOSC Quantico, VA location.

4.2.1.1 NetCOP – KEY ACTIVITIES The Contractor shall support the following key activities associated with NetCOP:

- Triage and classification of incidents and restoration of affected NetCOP systems to normal operation within response times specified on the PRS below and with minimal impact on system operation
- Provide user account administration and execute access controls for NetCOP systems
- Classify and fulfill service requests and work orders associated with NetCOP systems
- Implement approved configuration changes to NetCOP systems and associated software
- Implement maintenance and security patches to ensure the confidentiality, integrity, and availability of NetCOP systems and associated software
- Secure and/or harden NetCOP systems and software applications
- Develop reports and reporting capabilities specific to the tools and applications comprising NetCOP systems

- Execute performance tuning of NetCOP information systems and associated software applications and databases
- Design, review, and update the architecture of NetCOP systems
- Web style/skin design, data visualization, and graphic artistry of NetCOP systems
- Author, update, and sustain system design, configuration, and administration documentation (CDRL A00C).

4.2.1.2 NetCOP – EVENT MANAGEMENT SYSTEM The Contractor shall provide Event Management System (EMS) support, including the design, architecture, and implementation of increased capabilities within the enterprise event management tool set on both unclassified and classified enterprise network environments. The tool set is intended to facilitate the Marine Corps' ability to provide IT personnel across the Marine Corps with ability to monitor and manage the performance and availability of USMC services, systems, networks, and storage.

The Contractor shall support key activities associated with EMS support, including:

- Enhanced Monitoring capabilities, including the deployment of Operations Manager Smart Plug Ins for key USMC IT services such as Blackberry, Exchange, Active Directory, Database, Middleware, and Virtualization infrastructure services.
- Enhancements to HP Business Service Management (BSM) and Operations Manager I (OMi) to include development and implementation of Topology Based Event Correlation (TBEC) to aid in reducing Mean Time To Repair (MTTR).
- Implementation and configuration of HP Server Automation (SA), Network Automation (NA), and Operations Orchestration to automate functions of deployment, maintenance, configuration management, and, incident response for MCEN services and infrastructure.
- Enhanced HP Universal Configuration Management Database (UCMDB) discovery and mapping. Including the discovery of virtual infrastructure and other services and synchronization of HP BSM to populate the HP Run Time Service Model (RTSM)
- HP tools expertise to support the integration of HP tool set with BMC ITSM tool set, including UCMDB integration with the Atrium CMDB and HP OMi events into BMC Remedy.
- Enhanced Service Intelligence, including implementation and configuration of HP Service Health Reporter (SHR) for high level reporting on key MCEN services and infrastructure health. Additionally includes implementation and configuration of HP Virtualization Performance Viewer (VPV) to provide reporting and planning within virtual environments and other USMC IT services.
- Enhanced UCMDB discovery including systems, applications, and associated interrelationships and dependencies as well as creation of Service Maps.
- Implementation and configuration of HP Service Intelligence Analyzer (SHA) to provide analysis of Service Health and predictive capabilities in support of Service monitoring and management.
- Identify and replace regional legacy tool capabilities such as SolarWinds and CA Spectrum within MEMS.
- Provide early life support and assist in promoting adoption of newly implemented MEMS capabilities.

4.2.1.3 BMC TOOLS (REMEDY ITSM) ADMINISTRATION AND ARCHITECTURE SUPPORT

The Contractor shall be responsible for configuring aspects of the BMC tools deployed by NetCOP. The Contractor shall be responsible for configuring the following:
BMC ITSM Suite (Remedy) versions 8.1 or newer, Apache Tomcat 7.0.52 or newer, BMC Analytics version 7.6 or newer, and BMC Business Objects version 4.0 or newer software systems in a multi-tiered, highly available, enterprise environment. The current environment includes the use of Atrium CMDB, Atrium Integrator, Remedy User, Remedy Data Import, Remedy Developer Studio, and Remedy ITSM Process Designer tools to support this task. The environment consists of multiple instantiations of these systems in support of the unclassified, classified, and testing/integrations networks. The configuration tasks require capabilities in administration, troubleshooting, tuning, and architecting BMC tools in large-scale, global, environments. The Contractor shall develop custom workflows, forms, and applications using the identified tools. The Contractor shall be responsible for developing reports in both the built in Business Intelligence and Reporting Tools (BIRT) and the BMC Business Analytics system. Support tasks shall also include user support including account and access management, incident response, and responding to informational requests.

4.2.1.4 ENTERPRISE EVENT MANAGEMENT TOOLS ADMINISTRATION AND ARCHITECTURE SUPPORT

The Contractor shall be responsible for configuring to ensure proper functionality all of the aspects of the Event Management tools deployed by NETCOP (i.e. MEMS), including the following tools currently deployed:

- HP Business Service Management (BSM) 9.22
- HP Universal Configuration Management Database (UCMDB) 10.01
- HP Operations Manager (OMW) (includes HP Performance Manager 9.00) 9.00
- HP Network Node Manager i (NNMi) (including I Smart Plug-in (iSPI) for Performance Metrics) 9.24
- HP SiteScope 11.2
- HP Universal Discovery 10.01
- HP Service Health Reporter (SHR) 9.30
- HP Service Health Analyzer (SHA) 9.30
- HP Service Health Optimizer (SHO) 9.30
- HP Real User Monitor Engine (RUM) 9.22
- HP Diagnostics Commander 9.22
- HP Server Automation (SA) 10.01
- HP Operations Orchestration (OO) 9.07
- HP Network Automation (NA) 9.22 or newer version software system

The environment consists of multiple instances of these systems in support of the unclassified, classified, and testing/integrations networks. This support requires capabilities to support the integration of tools across distributed WANs, residing in large-scale, global, environments. Support tasks require capabilities in ITSM administration, troubleshooting, tuning, and architecting, and shall provide user support including account and access management, incident response, and responding to informational requests.

4.2.1.5 OPERATIONAL DIRECTIVES REPORTING SYSTEM SUPPORT

The Contractor shall be responsible for operating and maintaining the currently deployed system in accordance with required system uptimes, as well as perform full life cycle development activities ranging from development and implementation of minor enhancements to development and implementation of major version releases and revisions. The Contractor shall develop web based solutions and applications in a multi-tiered, highly available, enterprise environment utilizing the following:

- Microsoft C#
- Microsoft Asp.net
- Microsoft Visual Studio
- Microsoft .Net Entity Framework
- Microsoft SQL Server 2008 (or newer)
- Microsoft SQL Server 2008 Reporting Services (or newer)
- Microsoft IIS skills

The Contractor shall develop reports in both the web application front end and back end database technologies. The Contractor shall provide capabilities to support creating custom workflows, forms, and web applications. Support tasks include aspects of user support, such as account and access management, incident response, and responding to informational requests.

The Contractor shall be responsible for developing custom designs, visual layouts, and graphic art for the graphical user interfaces of systems supported by NETCOP. This support includes designing the layout and data visualization aspects of reports generated by NETCOP systems. The environment includes ASP.net C#, and requires capabilities in designing, creating, and implementing cascading style sheets for ASP.net web applications.

C.4.2.2 ASSURED COMPLIANCE ASSESSMENT SOLUTION (ACAS) SUPPORT

C.4.2.2.1 ACAS IMPLEMENTATION SUPPORT

All elements under this subtask shall be performed 8 hours per day, 5 days per week, 52 weeks per year (8x5x52) (Federal business days) at Quantico, VA. The Contractor shall support the Command in the design and implementation of ACAS solutions for all MCEN networks as well as train operators from MARFORs and internal Information Assurance personnel to maintain and operate the Secure Configuration Compliance Validation Initiative (SCCVI) tool functionality.

The Contractor shall:

- Rack and provision government furnished equipment (servers), install and patch operating systems, application, and document DISA STIGs applicable to each network environment for all ACAS implementations.
- Assess current ACAS implementations for each of the MCEN networks and recommend changes (CDRL A00M).
- Document the steps required to design the ACAS solution for each of the MCEN networks to include IP address, Fully Qualified Domain Name, and physical location of each component (CDRL A00M).

- Create network diagrams of the designs with Microsoft Visio (include list of hardware and software requirements) (CDRL A00M).
- Create reporting dashboard designs and reports for each environment that are specific to the following audiences: Leadership & Executives; Cybersecurity Staff; and System Administrators (CDRL A00M).
- Ensure MCEN networks receive periodic updates from either the DISA/DoD Patch Repository or Tenable.
- Implement the Reporting Dashboard designs and use reporting tool to create reports.

C.4.2.2.2 ACAS OPERATIONS, MAINTENANCE, AND TRAINING

The Contractor shall operate and maintain the ACAS solution, to support network and application scanning and configuration assessments are conducted and incidents are resolved in accordance with the incident response table in Section C.5 and MCNOSC SOPs . See above paragraph for required work hours.

The Contractor shall:

- Ensure scheduled scans are covering 100% of intended assets and are being run successfully.
- Maintain the Nessus scanners and PVS's connectivity with the associated Security Center (SC).
- Ensure SC is being updated either manually, via professional feed, or via a DISA-hosted feed.
- Address unsuccessful updates of the SC and identify the root cause of the unsuccessful update (corrected within four hours of discovery).
- Ensure anomalous activity identified by the PVS on each subnet/VLAN is reviewed and tasked to the incident handler, as appropriate, within two hours of identification of the anomalous activity.
- Develop and/or update the Standard Operating Procedures (SOP) to support each of the MCEN ACAS solutions documented within the Sharepoint Portal (CDRL A00C).

C.4.3 MCEN OPERATIONS SUPPORT

C.4.3.1 OPERATIONS CENTER SUPPORT

The MCNOSC Operations Center serves as the Systems Control Center for all USMC Enterprise Network systems. The Operations Center utilizes industry best practices in the ITIL v3 framework with a focus on Service Transition and Service Operations. The Operations Center is segmented into four primary groups which are overseen by one management element. The four groups in the Operations Center are: Watch Teams, Network Operations Center (NOC) Service Desk, IT Business Processes, and Operations Center Development. Each one of these sections is reliant on one another to be successful in the group's individual mission. **Required operational hours and locations are specified under each subtask.**

The following is historical workload data for the Operations Center:

Item Tracked	Quantity(Annual)
Incidents/Service Requests	88,500
Investigations	110
Electronic Spillages	80
AMHS messages released	3,415
E-mails received/handled	84,000
Tickets handled by the Service Desk	65,600
Web Site content management	1,500
Knowledge Management	168
Change records managed/processed for infrastructure	6,100
Release packages created	450
Problem Tickets/Investigations	107
Known Errors Created	50
Solutions Created	28
Daily Turnover Log	365
Executive Briefings	260
Situation Reports	485

For all subtasks under C.4.3, refer to the tables in Section C.5 for required response times and service target requirements.

Performance Standards and Acceptable Quality Level for C.4.3 See attached PRS below.

C.4.3.1.1 INFORMATION AND KNOWLEDGE FACILITATION, AND WEB CONTENT SUPPORT

As the Systems Control Center for the MCNOSC, the Operations Center must maintain positive control and understanding of information as it's reported and disseminated from and to our higher headquarter and fleet customers. **This task shall be performed 8x5x52 (Federal business days) on site at the Quantico, VA location.**

Information Management comes in a myriad of forms, and as such the Operations Center is required to publish information on a routine basis (i.e. shift reports, weekly roll-up reports, and monthly reports. See subsequent sections for more details on reporting). In order to perform this function MCNOSC must utilize numerous methods to transmit information such as operational message traffic, posting and development of informational websites, submission of knowledge articles, submission and archiving of organizational emails, creating blogs and streaming feeds, and other organization's online offerings for the IT community.

The Contractor shall:

- Assist in the creating of, and adherence to, an Operations Center information management plan.
- Ensure the knowledge database is maintained in accordance with Government policies and procedures and up-to-date to include initial and annual reviews.
- Populate the knowledge management database in accordance with Government policies and procedures.

- Facilitate meetings between IT technical support sections, to include producing agendas and meeting minutes for publication.
- Design websites to support the organization's strategies and goals relative to external customer and higher headquarters communications, using web development technologies such as SharePoint, Java, and HTML.
- Provide graphical design support by means of art, images and visual materials for mass communications, briefings, presentations, and informative and instructional material through a variety of media outlets and multimedia programs.
- Provide, manage, and perform website editorial activities including, gathering and researching information that enhances the value of the site.
- Provide web content development for the overall functionality of the MCNOSC Knowledge Management collaborative site that supports information gathering and decision-making.

C.4.3.1.2 WATCH TEAM SUPPORT

The MCNOSC Watch Teams serve as the eyes and ears of the MCEN. These teams prioritize and align resources to best meet the mission of the MCNOSC. **The Contractor shall support 24x7x365) real time analyses of all events and incidents as they occur on the network.** The Contractor shall also serve as a team consultant to the MCNOSC Battle Captain.
The Contractor shall serve as action officers and have knowledge of IT business processes. The Contractor shall use Event management tools, BMC Remedy, SharePoint, and Service Operations tools to perform this task. The Contractor shall perform troubleshooting to support networking, servers, and applications incident support. Each Contractor position on the Watch Team shall create a Daily Turnover Log entry in accordance with Watch SOPs. The Contractor shall provide Watch Team Work Updates (CDRLA00H) to the USMC TPOC or designee each week that outline work performed and work to be accomplished in the upcoming week. **The Contractor shall provide support from MCNOSC Quantico, VA location.**

The Contractor shall, in accordance with Watch Team SOPs to be provided upon award:

- Monitor, detect, and take immediate action on events and incidents as they occur on the network based on Watch Team operating procedures.
- Identify problems and take appropriate actions based on Watch Team operating procedures.
- Create Watch Team Formal Reports and assign work requests to the proper group based on Watch Team operating procedures (CDRL A00H).
- Collect and analyze events and incidents from multiple sources and correlating information between IT management tools based on Watch Team operating procedures.
- Advise the MCNOSC Battle Captain on the best business process to use to achieve desired results based on Watch Team operating procedures.
- Assist in the creation and distribution of on-demand Situation Reports as required.

C.4.3.1.2.1 WATCH CLERK SUPPORT

The Contractor shall provide 24x7x365 real time management of information flowing in and out of the MCNOSC Watch Team at the Quantico, VA location. Watch Clerks play an

integral role in allowing the MCNOSC Battle Captain to make the best possible decisions with available information. The Watch Clerk environment is supported by SharePoint and Remedy automated tools.

The Contractor shall, in support of the Watch Team:

- Manage, track, and file any and all information that the MCNOSC Watch Team receives and produces.
- Document all actions taken in order to resolve incidents on the enterprise network.
- Organize all MCNOSC Watch Team data based on team procedures.
- Filter information quickly and easily to gain important information necessary for the MCNOSC Battle Captain to make decisions.
- Provide Watch Team Reports to the MCNOSC Battle Captain and Executive Staff (CDRL A00H).
- Produce executive level Watch Team Briefings for MCNOSC.

C.4.3.1.3 NOC SERVICE DESK SUPPORT

The NOC Service Desk manages and coordinates the handling of Tier III Enterprise incidents, problems, and requests with users and IT groups for unclassified and classified equipment in support of a government Lead. Note: Tier III support is defined as a very specialized job performed by the specialists who were usually involved in the product development. Tier I and Tier II support will typically be handled at the local and regional offices (MITSCs). The NOC service desk also serves as Tier I and II back up for the MITSC's and local offices after hours or when they are experiencing a shortage in staffing. Tier – I/Level 1 support is the basic level of customer support. The customer representative is a generalist with a broader understanding of the product, but might not understand the inner workings of the system. Tier-II level support involves technical knowledge and the desk is staffed by more experienced technicians who have strong exposure to troubleshooting. The Service Desk provides multiple means such as single toll-free number and single Web interface, for service and manages the life cycle of incidents, problems, events, and service requests including fulfillment, verification, and closure. The Service Desk communicates continually throughout the life cycle with users and IT groups, and continually utilizes and enhances of the Service Desk knowledge data base. The NOC environment is supported by ticketing tools (e.g., BMC Remedy) and event monitoring tools (e.g., Hewlett Packard) to **provide and manage the 24x7x365 Tier III Enterprise service desk support. The Contractor shall distribute approximately 80% of enterprise service desk support at Quantico, VA and 20% at Kansas City, MO.**

The Contractor shall:

- Provide Service Desk services to all MARFORs IT groups for unclassified and classified services.
- Monitor ticket submission and tracking through multiple means such as single number and single Web interface.
- Perform start to finish event management, including monitor Event Consoles for Events that require action, initiating Incidents and RFCs as required. Analyze Event records to detect trends, Document, assess, track, resolve, and fulfill Service Desk incidents,

problems, events, and requests in accordance with the documented Incident Management and Problem Management processes.

- Coordinate with the MCNOSC Watch Teams and Government representatives to resolve events, incidents and problems in accordance with the Event Management, Incident Management and Problem Management processes such as anomalies that affect more than one user.
- Coordinate with the Government civilians, Marines, and third party Contractors to resolve Network events, incidents and problems to include Install Move, Add, and Changes services for the customer; and to resolve Network connectivity anomalies.
- Recommend enhancements to the Event Management, Incident Management, and Problem Management Standard Operating Procedures.
- Assess equipment remotely, when possible, to resolve incidents, perform reconfiguration, and push software.
- Operate the on-line status system to initiate, query, track, update, and display Information, (such as aging and backlog) pertaining to incidents, problems, and service requests.
- Track the resolution of MCNOSC incident tickets as required.
- Verify resolution with the customer prior to resolving the ticket.
- Provide the USMC TPOC with a Post-Incident Report (CDRL A00J) regarding the reason for the outage, corrective actions taken, and any follow-on actions upon resolution of a trouble ticket for outage of service.
- Recommend and implement a customized priority process for service requests from deployed forces within the existing ticketing system.
- Generate, post, and retain historical information for weekly and monthly Service Desk performance measurements on a Government designated website and report this information as part of the Weekly and Monthly In-Progress Review (CDRL A00K).
- Process, manage, and execute classified and unclassified service requests.
- Provide users technical assistance and guidance to resolve service delivery issues.

C.4.3.1.4 IT BUSINESS PROCESS MANAGEMENT SUPPORT

Operations Center Business Process Management supports the maintenance and documentation of information management strategies to include Cyber Operations and Defense standard operating procedures, Marine Corps systems efficiency review, and continual Marine Corps Enterprise Network development to be employed by MCNOSC Operations Center personnel. It also supports the implementation and management of the ITSM processes as implemented by the MCNOSC. These currently include Incident and Service Request Management, Changes and Release Management, Event Management, and Problem Management. **The Contractor shall provide support from MCNOSC Quantico, VA location during normal business hours (8x5x52) (Federal business days).**

The Contractor shall:

- Analyze and reengineer the processes, with an understanding of technical problems and solutions as they relate to the current and future business environment.
- Conduct full Business Process Reviews and recommend and facilitate changes to business process that align to continuous service improvement initiatives.

- Coordinate meetings between IT technical support sections, to include producing agendas, sending meeting invitations, and producing meeting minutes.
- Conduct Business Process Audits to ensure adherence to IT management policies and procedures.
- Maintain the Operations Center collaborative site to coordinate planning, documentation, and training.
- Develop and administer a Training and Exercise Employment Plan (TEEP) that clearly outlines the major milestones directed by Operations Center management in accordance with Force Order (FORO) 3502.1.
- Determine estimated costs to the user of lost IT services.
- Identify and document areas of improvement in IT management on Marine Corps Enterprise Network in a MCEN Business Process Improvement Report.
- Develop business case analysis/analysis of alternatives to recommend and develop courses of action which best meet the USMC missions and needs.
- Draft and perform audits and updates of current and purposed IT management policies and procedures utilizing best business practices.

C.4.3.1.5 QUALITY CONTROL SUPPORT

The Contractor shall provide administrative and analytical support services related to computer networks and/or telecommunications with primary knowledge requirements associated with Quality Assurance. Contractor shall use Quality Control processes to review existing performance and recommend process improvements to improve performance metrics. The success of the Contractor in this area is dependent on the ability to properly identify and measure those ITSM Processes implemented by the MCNOSC. **The Contractor shall provide support from MCNOSC Quantico, VA location during normal government business hours (8x5x52) (Federal business days).**

The Contractor shall:

- Support and document an established Quality Control process using the Deming cycle, i.e., the Plan, Do, Check, Act (PDCA). This process should focus on identifying root causes or deficiencies in service operations.
- Document specific levels of quality that need to be achieved and how those objectives will be measured Based upon the applicable service level requirements.
- Collect data from the ITSM system and end users for the ITSM processes implemented by USMC. These include but are not limited to Incident Management, Change Management, Problem Management and Knowledge Management.
- Review and analyze collected data comparing it to expected level of quality listed in the attached PRS and SOPs.
- Determine the differences between expected and achieved levels of quality, determine their root cause, identify service deficiencies and recommend courses of action that will improve the process being reviewed.
- Develop and provide leadership with scheduled Quality Assurance Reviews that identify whether service quality is being met IAW performance requirements established in the PRS.

C.4.3.1.6 INCIDENT AND SERVICE REQUEST MANAGEMENT SUPPORT

The Contractor shall provide administrative and analytical duties related to computer networks and/or telecommunications with primary knowledge requirements of Incident and Service Request Management. To achieve this objective, Contractor shall ensure the incident and service request management Standard Operation Procedures (SOPs) and system workflows are being closely adhered to as the technicians work through the requests. The environment is supported by BMC Remedy, Crystal Reporting, and BMC Analytics. **The Contractor shall provide support from the Kansas City, MO location during normal business hours (8x5x52) (Federal business days).**

The Contractor shall:

- Act as a point of contact for all MCNOSC IM process activities
- Conduct technical and non-technical reviews of incident management procedures and recommend process improvements.
- Identify and report on trends and potential problem sources by reviewing incident and problem analyses.
- Track and manage all open incidents within the MCNOSC.
- Interfacing with Battle Captains and Queue Managers for the purpose of ensuring adherence to performance standards and resolution of Incidents/Service Requests in accordance with required response times.
- Develop and provide Detailed Incident and Service Request Management Reports with a primary focus on Critical Success Factors and Key Performance Indicators.
- Document and update all incident records; coordinate incident response actions between the MCNOSC and other Marine Corps offices and defense intelligence groups.
- Report on customer service metrics.
- Coordinating with MCNOSC Section level Queue Managers on Incidents/Service Requests as required.
- Identify and recommend Incident Management training requirements based on process improvement recommendations or identified areas requiring improvement.

C.4.3.1.7 CHANGE/RELEASE AND DEPLOYMENT MANAGEMENT SUPPORT

The Contractor shall provide Change Management and Release and Deployment Management functions. The Contractor is responsible for customer support and change, release and deployment best practices. **The Contractor shall provide 8x5x52 support during the standard work week Federal business days) . The Contractor shall provide support from MCNOSC Quantico, VA location.**

The Contractor shall:

- Ensure Requests for Change (RFC) submitted are valid, complete, and accurate.
- Perform risk and impact assessments on all submitted RFCs.
- Ensure all approved RFCs are prioritized correctly based on government direction.
- Assist in the initiation, tracking and facilitating post implementation review of completed RFCs as needed.

- Assist in development of release manifest's and project plans within BMC Remedy in support of enterprise level projects.
- Ensure all approved RFCs are associated to an appropriate release record within BMC Remedy when required.
- Ensure that the forward schedule of change is up-to-date and accurate. This may include schedules in multiple locations, to include BMC Remedy and Microsoft Sharepoint.
- Participate in USMC regional and enterprise change activities as needed.
- Coordinate with regional change and release managers/coordinators as needed.
- Participate in ITSM process initiatives and process reviews.
- Draft Operational Advisories for release.
- Monitor each RFC throughout its entire lifecycle.
- Assist the organizational liaison for all approved RFCs.
- Coordinate with and assisting the organization and external agencies for all RFCs and any issues that fall within the Change Management and Release and Deployment Management functions, as defined by the organization.
- Ensure all Change Management and Release and Deployment Management processes and procedures are adhered to by the organization and external agencies; provides input into important decisions regarding Change Management and Release and Deployment Management supporting technology requirements and process improvement.
- Raise change-related issues to the required level of management.

C.4.3.2 ENTERPRISE DIRECTORY AND MESSAGING (EDM) SUPPORT

Enterprise Directory and Messaging (EDM) is a collection of technology management teams, support teams and an escalation/triage team. EDM consists of the following core technology management teams that are referred to as "Product Groups" (PGs): Platforms, Messaging, Enterprise Cloud Infrastructure Services (ECIS), Database Administration (DBA), and Application Management. The support teams within EDM include Cybersecurity, Operational Management, and EDM Triage. Within each PG there are numerous technologies and services, managed and operated by EDM which are the objective of this subordinate task order to support. The Contractor shall provide technical support to operate, troubleshoot, and scale three separate domains with completely separate infrastructure and services. Each environment requires isolated access, patching, and security postures. **The uptime of all enterprise services is 99.97%, not including system maintenance.** The MCNOSC utilizes ITIL v 3.0 (and later versions) processes as general guidance for EDM support. The average mean time to resolve tickets is listed in the Watch Officer Key Performance Indicator Policy and the PRS and Service Target Requirements. All patching and Information Assurance Vulnerability Alert compliancy has to be accomplished on all Enterprise services in accordance with the MCNOSC change policy and within a six-day window of guidance without a patching solution.

The Contractor shall participate in a weekly status meeting and provide input on a weekly basis on EDM trends, incidents, incident resolution, and availability of services to the MCNOSC TPOC via a written EDM Status Report (CDRL A00A). The Contractor shall also provide EDM Meeting Minutes (CDRL A008) to the MCNOSC TPOC within one business day after the status meeting.

C.4.3.2.1 EDM ACTIVE DIRECTORY (AD) SUPPORT

The EDM AD Support team supports over 265,000 user accounts and 140,000 computer accounts across several AD domains on USMC's operated networks. The services that the AD Support team supports in Active Directory include accounts and group management, security configuration of the AD infrastructure, Domain Name Service (DNS), Dynamic Host Configuration Protocol, Distributed File Replication Services, Group Policy Object's and other directory services technologies as applicable.

The Contractor shall provide Tier III level Active Directory support. Tier III EDM AD support requires knowledge of the Windows Server Operating System and relevant AD applications (such as Lync, System Center Suite, Exchange). The underlying infrastructure consists of both physical servers and VMware based servers which requires knowledge in VMware Virtualization and VMware vCloud to perform the specialized EDM Active Directory tasks. **This task shall be performed 8x5x52 (Federal business days) on site at the Quantico, VA location.**

The Contractor shall:

- Maintain the overall health of technologies associated with AD and internal DNS.
- Resolve Active Directory tickets escalated from the service desk including the administrative activities and provide an EDM weekly Messaging Status Report (to be incorporated into the EDM Weekly Status Report, CDRL A00A).Coordinate incident tickets between Tier II and III sections as well as other sections as required. See Attachments A and F for required response times.
- Provide documentation, guidance and instruction to the Tier II and service desks for handling standard Active Directory related incidents, work orders and service requests.
- Provide Active Directory Service Desk Resolution Reports documentation to the service desk on the procedures for completing the task.
- Submit and execute AD related Request for Change tasks.
- Monitor the system availability and performance of AD with MCNOSC-provided event management tools and make corrective actions to incidents that lower the health of AD.
- Provide MCNOSC project support for AD related technologies.
- Coordinate with the Plans Division and other MCNOSC sections on AD-related issues.
- Support change management process; submit requests through Change Approval Board; participate in a Change Review Board.
- Escalate product issues that cannot be resolved internally to third party product vendors.
- Implement monitoring tool thresholds and conduct proactive event remediation.
- Provide analysis and remediation for DISA Security Technical Implementation Guidelines (STIG) for all responsible technologies in preparation for annual Commanders Cyber Readiness Inspections (CCRI).

C.4.3.2.2 EDM SECURITY APPLICATION FRONT END SUPPORT (SUCH AS TMG, F5, AND SIMILAR TECHNOLOGY)

The Contractor shall provide Tier III level Security Application Front End support. The Contractor shall configure Microsoft Threat Management Gateway (TMG) servers for access from the internet to internal Marine Corps application servers. The Contractor shall provide capabilities in supporting Boundary Security Devices, Active Directory, and firewalls to provide TMG and Wireless Application Protocol (WAP) services. The Contractor shall configure the

TMG services to support Windows Server, Exchange, SharePoint, networking, PKI/SSL and other technologies as applicable. Contractor personnel supporting TMG services shall be compliant with DoD-8570 TECH-III Level certifications. The infrastructure is a mixed environment of VMware based and physical based servers. These tasks require capabilities in VMware Virtualization, and VMware vCloud to perform the specialized EDM Boundary Security Device tasks. **This task shall be performed 8x5x52 (Federal business days) on site at the Quantico, VA location.**

The Contractor shall:

- Maintain the overall health of technologies associated with Gateway and Firewall Services.
- Provide support for Gateway and Firewall related technologies.
- Monitor the health of Gateway and Firewall Services with Government-provided event management tools.
- Resolve TMG tickets escalated from the service desk and provide an EDM weekly Messaging Status Report (to be incorporated into the EDM Weekly Status Report, CDRL A00A) in accordance with required response times.
- Provide documentation, guidance and instruction to the Tier 1 service desk for handling standard Gateway and Firewall Services related incidents, work orders and service requests.
- Submit and execute Gateway and Firewall Services related Request for Change (RFC) tasks.
- Coordinate incident tickets between Tier II and III sections as well as Engineering and other sections.
- Support the change management process by submiting requests through Change Approval Board, participating in a Change Review Board, and providing information to support decision making.
- Escalate issues to third party product vendors.
- Implement monitoring tool thresholds and conduct proactive event remediation.
- Monitor and implement, upon management approval, guidance from the USCYBERCOM.
- Configure Secure Socket Layer access and logging on the devices.
- Provide analysis and remediation for DISA Security Technical Implementation Guidelines (STIG) for all responsible technologies in preparation for annual Commanders Cyber Readiness Inspections (CCRI).

C.4.3.2.3 EDM MESSAGING SUPPORT

The contractor shall provide Tier III level Messaging support. The Contractor shall configure aspects of the Microsoft Enterprise Exchange organization in support of a 265,000 user environment across all AD domains on MCEN to provide messaging support. The EDM messaging environment consists of Microsoft Exchange mail services (Client Access, Hub Transport, and Mailbox server roles), Enterprise Blackberry services, Cisco E-mail security solutions, NetApp backup and restore solutions, and UnitySync directory synchronization services. The underlying infrastructure consists of physical servers, VMware Virtualization and NetApp storage solutions. **This task shall be performed 8x5x52 (Federal business days) on site at the Quantico, VA location.**

The Contractor shall:

- Maintain the overall health of technologies associated with EDM Messaging.
- Provide Microsoft Enterprise Exchange operational configuration management support.
- Provide Blackberry Enterprise Server Version 5+ (v12) technical expertise in the management, maintenance, and problem resolution. Including Blackberry IT policy and configuration management.
- Provide Cisco IronPort technical expertise in the management, maintenance, and problem resolution.
- Provide Directory Support for the following products: ADLDS, Unity Sync, and Identity Integration Feature Pack, Forefront Identity Manager to manage the USMC Global Address List (GAL).
- Resolve EDM messaging tickets escalated from the service desk including the administrative activities for: message tracking, content filter tasks, and reporting and provide an EDM weekly Messaging Status Report (to be incorporated into the EDM Weekly Status Report, CDRL A00A) in accordance with required response times.
- Configure Antivirus products and HBSS as they relate to Exchange Servers.
- Provide guidance and instruction (to include written documentation) such as SOPs and inputs into the knowledge management system repository to the service desk for handling standard Message related incidents and service requests.
- Provide documentation, guidance and instruction to the Tier 1 service desk for handling standard Messaging related incidents, work orders and service requests.
- Submit and execute EDM Messaging related change request tasks.
- Coordinate incident tickets between Tier II and III sections as well as other sections as required.
- Monitor the health of EDM Messaging with MCNOSC-provided event management tools.
- Provide MCNOSC project support for EDM Messaging related technologies.
- Coordinate with the Plans Division and other MCNOSC sections on EDM messaging issues.
- Support change management process; submit requests through Change Approval Board; participate in a Change Review Board.
- Escalate product-related issues to third party product vendors.
- Implement monitoring tool thresholds and conduct proactive event remediation.
- Ensure that any latency, whether at the Command or the Forward Operating Bases (FOBs) level, is identified and mitigated/remediated upon discovery in accordance with required response times.
- Monitor availability of system upgrades.
- Provide analysis and remediation for DISA Security Technical Implementation Guidelines (STIG) for all responsible technologies in preparation for annual Commanders Cyber Readiness Inspections (CCRI).

C.4.3.2.4 EDM VIRTUALIZATION SUPPORT (VM)

Within EDM's ECIS team reside multiple sub section that provide operations and management of the MCEN's virtual and storage infrastructure services. The contractor shall provide Tier III

level Virtualization support. The Contractor shall configure aspects of VM in support of a 265,000 user environment across all domains on USMC operated networks. EDM Virtualization support requires knowledge of VMware and the experience to deploy and maintain complex VMware environments. The EDM environment is supported by VMware Update Manager, VSphere, ESXi, storage area networks, SnapManager, Windows Server operating systems, VMware vCloud and adheres to DISA Standard Technical Implementation Guidance. In addition, the Contractor shall work with MCNOSC customers and product vendors on configuration of features and functionality; document best practices and internal processes for internal training; assist with change management and documentation of environments; work with a dedicated team to ensure success of select customer groups, including VIPs; and ensure customer uptime through precise monitoring implementations, good change management, and incorporation of best practices. **This task shall be performed 8x5x52 (Federal business days) on site at the Quantico, VA location.**

The Contractor shall:

- Maintain the overall health of technologies associated with Virtual Infrastructure (VI), including performing required system maintenance to ensure system availability and security performance.
- Resolve EDM VM tickets escalated from the service desk including the administrative activities and provide an EDM weekly Messaging Status Report (to be incorporated into the EDM Weekly Status Report, CDRL A00A).
- Provide documentation, guidance and instruction to the Tier 1 service desk for handling standard Virtual Infrastructure related incidents, work orders and service requests.
- Provide guidance and instruction to the service desk for handling standard virtual infrastructure (VI) related incidents and service requests.
- Submit and execute VI related Request for Change (RFC).
- Coordinate incident tickets between Tier II and III sections as well as other sections as required.
- Monitor the health of VI with MCNOSC provided event management tools.
- Provide MCNOSC project support for VI related technologies.
- Coordinate with the Plans Division and other MCNOSC sections on EDM VM issues.
- Support change management process; submit requests through Change Approval Board; participate in a Change Review Board.
- Escalate issues to third-party product vendors for resolution support.
- Implement monitoring tool thresholds and conduct proactive event remediation.
- Provide analysis and remediation for DISA Security Technical Implementation Guidelines (STIG) for all responsible technologies in preparation for annual Commanders Cyber Readiness Inspections (CCRI).

C.4.3.2.5 EDM STORAGE AREA NETWORK (SAN) SUPPORT

Within EDM's ECIS team reside multiple sub section/technology areas that provide operations and management of the MCEN's virtual and storage infrastructure services to include maintaining the backup and recovery services. The contractor shall provide Tier III level Storage Area Network (SAN) support. The Contractor shall configure all of the aspects of the SAN hardware and software within the installation. The EDM SAN support includes Snaps

(snap mirror and snap vaulting), storage provisioning, management software, recovery procedures, hardware installation and security of Logical Unit Numbers (LUNS) and access to each LUNS.

The configuration support requires knowledge of storage filers, software and hardware at the Tier III Level and Windows, VMware, and networking technology. The environment is VMware based. The environment utilizes fiber technologies in which zoning methodology is required to manage. The environment also utilizes ISCSI technology in which the iGroup management methodology is required. **This task shall be performed 8x5x52 (Federal business days) on site at the Quantico, VA location.**

The Contractor shall:

- Maintain the overall health of technologies associated with Storage Area Networks.
- Provide a NetApp Resident onsite support.
- Resolve EDM SAN tickets escalated from the service desk including the administrative activities and provide an EDM weekly Messaging Status Report (to be incorporated into the EDM Weekly Status Report, CDRL A00A) in accordance with required response times.
- Provide SAN Capacity Reports and Performance Metrics (CDRL A00B) on a monthly basis.
- Provide documentation, guidance and instruction to the Tier 1 service desk for handling standard Storage Area Network (SAN) related incidents, work orders and service requests.
- Provide guidance and instruction to the Tier I organizations for handling standard SAN related incidents and service requests.
- Provide EDM SAN documentation to Tier I organizations on the procedures for completing the task.
- Submit and execute SAN related Request for Change (RFC) tasks.
- Coordinate incident tickets between Tier II and III sections as well as other sections as required.
- Monitor the health of SANs with MCNOSC- provided event management tools.
- Provide MCNOSC project support for SAN related technologies.
- Coordinate with the Plans Division and other MCNOSC sections on EDM SAN issues.
- Support change management process; submit requests through Change Approval Board; participate in a Change Review Board.
- Escalate product issues to third party product vendors.
- Implement thresholds to monitor tools and conduct proactive event remediation.
- Work closely with the MCNOSC management to continually improve the SAN performance while recommending solutions that reduce the overall Total Cost of Ownership (TCO) and increase the MCNOSC Return on Investment (ROI) on the SAN investment.
- Provide analysis and remediation for DISA Security Technical Implementation Guidelines (STIG) for all responsible technologies in preparation for annual Commanders Cyber Readiness Inspections (CCRI).

C.4.3.2.6 EDM CONFIGURATION MANAGEMENT

Within the EDM's Application Management team reside multiple sub section/technology areas that provide operations and management of the MCEN's enterprise server and workstation systems to include configuration and patch management. The contractor shall provide Tier III Configuration Management support. The Contractor shall establish and maintain the Microsoft Systems Center Suite of tools and IBM Big FixEndpoint Manager (IEM) (Commonly referred to as Big Fix) to support the Enterprise from the workstations and users to servers and solutions. The Contractor shall install Management Servers, Agents, reporting servers, and data warehouses where necessary and configure rules and alerts consistent with the support structure.
The Contractor is responsible for the operation of the MCEN Microsoft System Center Operations Manager (SCOM) Configuration Manager (SCCM), Orchestrator (SCORCH), IBM Endpoint Manager, Dell Change Auditor, Dell GPO Admin, and Dell Recovery Manager in an enterprise environment containing more than 100,000 users. The configuration environment consists of Windows Server, Exchange, SharePoint, BMC Remedy, networking, PKI and SSL and support of the products for the EDM Management Support as well as enabling the System Center Suite and Big Fix to be accessible for self service and distributed administration of users and devices. The infrastructure is a mixed environment of VMware based and physical based servers. The Contractor must possess expertise in VMware Virtualization, and VMware vCloud to perform the specialized EDM configuration management tasks. **This task shall be performed 8x5x52 (Federal business days) on site at the Quantico, VA location.**

The Contractor shall:

- Maintain the overall health of technologies associated with Configuration Management.
- Resolve all Configuration Management tickets escalated from the service desk including the administrative activities and provide an EDM weekly Messaging Status Report (to be incorporated into the EDM Weekly Status Report, CDRL A00A).
- Provide documentation, guidance and instruction to the Tier 1 service desk for handling standard Event and Configuration Management related incidents, work orders and service requests.
- Submit and execute Event Management related Request for Change (RFC) tasks.
- Coordinate incident tickets between Tier II and III sections as well as other sections as required.
- Monitor the health of Event Management Infrastructure with MCNOSC provided event management tools.
- Provide MCNOSC project support for Configuration Management related technologies.
- Coordinate with the Plans Division and other MCNOSC sections on Configuration Management issues.
- Support change management process; submit requests through Change Approval Board; participate in a Change Review Board.
- Escalate product issues to third party product vendors upon Government approval.
- Implement monitoring tool thresholds and conduct proactive event remediation.
- Provide analysis and remediation for DISA Security Technical Implementation Guidelines (STIG) for all responsible technologies in preparation for annual Commanders Cyber Readiness Inspections (CCRI).

C.4.3.2.7 EDM MICROSOFT SELF SERVICE PORTAL SUPPORT

Within the EDM's Application Management team reside multiple sub section/technology areas that provide operations and management of the MCEN's enterprise server and workstation systems to include automating enterprise tasks. The contractor shall be responsible for operating and maintaining the currently deployed system as well as full lifecycle development activities ranging from development of minor enhancements to development of major version releases and revisions. The contractor shall develop web based solutions for ITSM technology automation and service delivery focusing on the development of the System Center Service Manager (SCSM) platform. The Contractor will provide Tier III level SCSM support. The Contractor shall be responsible for the configuration of System Center Service Manager, and SSL access and web services on these devices. Web services and configuration support involves Structured Query Language (SQL), Active Directory (AD) and Web technologies at the Tier III level and Windows Server, Public Key Infrastructure (PKI), and Secure Socket Layer (SSL). The environment is supported by VMware based technology. **This task shall be performed 8x5x52 (Federal business days) on site at the Quantico, VA location.**

The following is the skillset the government anticipates will be needed to meet the requirements of this subtask:

- Understanding of Microsoft Management Platforms and roadmaps.
- Understanding of Microsoft Technology stack.
- SCSM & Orchestrator Administration
- Experience with System Center Operations Manager.
- Solid understanding of Microsoft System Center 2012 components with a strong focus on Service Manager and how it integrates with the other suite components.
- Service Manager Authoring, in combination with designing and integrating with run books in Orchestrator.
- Experience in Orchestrator integration packs.
- Experience in Model / class based architecture in SCSM
- Extensive PowerShell / Scripting experience
- Experience with Internet Information Service (IIS) and HyperText Markup Language (HTML)
- Experience with PKI

The Contractor shall:

- Maintain the overall health of technologies associated with Service Manager.
- Configure connectors and integrate products such as Orchestrator, Operations Manager, Active Directory, and Configuration Manager with Service Manager.
- Support the integration of third-party web front for Service Manager.
- Resolve EDM SCSM/SCORCH incident tickets escalated from the service desk including the administrative activities and provide an EDM weekly Messaging Status Report (to be incorporated into the EDM Weekly Status Report, CDRL A00A).
- Provide documentation, guidance and instruction to the Tier I service Desk for handling standard SCSM related incidents, work orders, and service requests.
- Prepare, submit, execute, and track all Service Manager related Requests for Change (RFC) tasks.
- Coordinate incident tickets between Tier II and III sections as well as other sections as required.

- Monitor the health of SCSM architecture with MCNOSC provided event management tools.
- Provide MCNOSC project support for SCSM/ITSM/Automation related technologies.
- Coordinate with Plans Division and other MCNOSC sections on SCSM issues.
- Support and provide automation for change management process: Submit requests through Change Approval Board: Participate in a Change Review Board.
- Escalate issues to third party product vendors upon Government approval.
- Implement monitoring tool thresholds and conduct proactive event remediation.
- Provide analysis and remediation for DISA Security Technical Implementation Guidelines (STIG) for all responsible technologies in preparation for annual Commanders Cyber Readiness Inspections (CCRI).

C.4.3.2.8 EDM DATABASE SUPPORT (DBA)

The contractor shall provide Tier III level DBA support. The Contractor shall be responsible for the configuration of all databases to include Microsoft SQL databases, throughout USMC application servers. The Contractor shall configure SSL access and logging on the devices. The environment is currently supported by VMware. **This task shall be performed 8x5x52 (Federal business days) on site at the Quantico, VA location.**

The Contractor shall:

- Maintain the overall health of technologies associated with Database Infrastructure.
- Resolve all EDM DBA incident tickets escalated from the service desk including the administrative activities and provide an EDM weekly Messaging Status Report (to be incorporated into the EDM Weekly Status Report, CDRL A00A).
- Provide documentation, guidance and instruction to the service desk for handling standard network infrastructure related incidents and service requests.
- Submit and execute network related change request tasks.
- Coordinate incident tickets between Tier II and III sections as well as other sections as required.
- Monitor the health of Database Infrastructure with MCNOSC provided event management tools.
- Provide MCNOSC project support for Database Infrastructure related technologies.
- Coordinate with the Plans Division and other MCNOSC sections on DBA issues.
- Support change management process; submit requests through Change Approval Board; participate in a Change Review Board.
- Escalate product-related DBA issues to third party product vendors.
- Implement monitoring tool thresholds and conduct proactive event remediation.
- Provide analysis and remediation for DISA Security Technical Implementation Guidelines (STIG) for all responsible technologies in preparation for annual Commanders Cyber Readiness Inspections (CCRI).

C.4.3.2.9 EDM ENTERPRISE ARCHITECTURE SUPPORT

The Contractor shall be responsible for supporting technical approaches and interdependencies between the Enterprise level servers. Provide technical guidance to the Product Groups and support team in resolving enterprise challenge and implementing new overlapping technologies. The contractor shall work with teams to develop the workforce and ensure interdependencies and

risks are identified and resolved prior to affecting system availability or network performance. The Contractor shall support the analysis of technical architecture and report (CDRL A00D) all findings to the Enterprise Directory and Messaging leadership (to be incorporated into the EDM Weekly Status Report, CDRL A00A). **This task shall be performed 8x5x52 (Federal business days) on site at the Quantico, VA location.**

The Contractor shall:

- Provide technical oversight of all activities performed by third party contractor personnel.
- Provide EDM subject matter expertise in Microsoft technologies to include but not limited to Active Directory and MS Exchange.
- Assess the operational requirements to make architectural recommendations aligned with the MCNOSC enterprise strategic vision and present to leadership.
- Coordinate with global teams via telephone and video conferences on technical operations issues that impact the MCNOSC Enterprise.
- Develop and maintain a Work Breakdown Structure (WBS) for EDM technical initiatives.
- Monitor and review the success of technical projects and ensure that the technical projects are meeting cost, schedule, and scope requirements and follow the USMC's architecture guidance.
- Provide Architecture Presentations and Architecture Technical Documentation to MCNOSC operations senior leadership.
- Conduct periodic Architecture Site Assessments and provide an Architecture Site Assessment Report for each assessment completed to include findings and recommendations.
- Provide network and system architecture guidance and training on technical environment to MCNOSC operations staff members.
- Leverage enterprise architecture support to troubleshoot complex computer system issues.

C.4.3.2.10 EDM TRIAGE SUPPORT

The EDM Triage Team is the forefront of EDM, providing Tier II support in incident and event management. As stated in previous sections EDM supports over 265,000 user accounts and 140,000 computer accounts across several AD domains on USMC's operated networks. This team is responsible for the day to day operation and support for all of EDM's technologies listed above. This effort includes the initial identification and troubleshooting of outages and rapid resolutions to enterprise level outages. This effort also includes the providing escalated troubleshooting support from subordinate and regional Marine Corps Units. **This task shall be performed onsite 24x7x365 at the Quantico, VA location.**

The Contractor shall:

- Maintain the overall health of technologies associated with EDM.
- Resolve Active Directory tickets escalated from the service desk including the administrative activities and provide an EDM weekly Messaging Status Report (to be incorporated into the EDM Weekly Status Report, CDRL A00A).

- Develop and maintain supporting documentation to improve success rates in completing service requests and incident resolutions. To include (but not limited to) templates, desktop procedures, knowledge base archives, and turnover logs.
- Monitor the health of All EDM systems with MCNOSC-provided event management tools and make corrective actions to incidents that lower the availability of enterprise system services.
- Support change management process; submit requests through Change Approval Board; participate in a Change Review Board. Specifically coordinate EDM maintenance to ensure all changes are known and reported to prevent erroneous reports of outages and reduce troubleshooting time for failed maintenance.
- Escalate product issues to product groups.
- Implement monitoring tool thresholds and conduct proactive event remediation.

C.4.3.3 INTEGRATED NETWORK SUPPORT (INS)

The objective of Integrated Network Support (INS) is to manage the Information Assurance (IA) boundary architecture for the garrison and tactical MCEN while ensuring compliance with the and DISA published technical guidance and higher operational standards; to provide customized on-site training and tactical network support to the Marine Corps Operational Forces; to provide Marine Corps unified communication capabilities to the Marine Corps Operational Forces to include Voice Over Internet Protocol (VOIP), Voice Over Secure Internet Protocol (VOSIP), and Video Teleconferencing (VTC). The INS section utilizes industry best practices in the ITIL v3 framework with a focus on Service Transition and Service Operations.

The MCEN consists of tactical networks, networks deployed aboard ships, and garrison networks aboard camps and stations. At its highest tier, the MCEN is interconnected to the Global Information Grid (GIG), a globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. Regional access to the Defense Information System Network (DISN) and its component networks, such as, the Non-secure Internet Protocol Router Network (NIPRNet), and the Secret Internet Protocol Router Network (SIPRNet) is also provided. The INS Tier III section provides support for approximately 300 classified and un-classified garrison and deployed tactical Information Assurance (IA) boundary suites (about 25 at a given time) around the world and the WAN links that connect those sites to each other and to DISA.

Directives applicable to the performance of the INS work are as follows:

- DoD 8570
- DoD 8500
- DISA CIRCULAR 300-115-3
- DISA STIGS
- MCNOSC Desktop Procedure D03-502
- MCNOSC Order 3100 (CCIR)
- MCNOSC Order 3020.1 (COOP)
- Headquarters Marine Corps, C4, Enterprise Security Directives
- DISA Connection Approval Process (DISA CAP)

- DISA Circulars
- INS Desktop Procedures and policies

The following Hardware (H/W) and Software (S/W) platforms are supported within INS:

WAN Optimization Support	H/W: Riverbed Steelhead, F5 Load Balancers
Video Teleconferencing and Voice over Internet Protocol Support	S/W-H/W Not vendor specific
Domain Name System (DNS) Support	H/W: Rack Server, Laptop S/W: Red Hat Enterprise Linux, RHEL Syslog
Firewall Support	H/W: ACME Packet; Cisco ASA; FortiNet FortiGate; McAfee Sidewinder; Juniper NetScreen, ISG, SSG S/W: FortiOS, CISCO IOS, NXOS; SecureOS; ScreenOS, JUNOS
Router Support	H/W: Cisco, Juniper, Brocade S/W: Cisco IOS, NXOS; JUNOS, FOS
Switch Support	H/W: Juniper, Cisco, Ericson, ForeSystems, Brocade S/W: JUNOS; CISCO IOS, NXOS, FOS
Web Content Filtering Support	H/W: BlueCoat S/W: BlueCoat
WAN Optimization Support	H/W: Riverbed Steelhead

C.4.3.3.1 INS SUPPORT TIER III

INS Tier III serves as the Subject Matter Expert (SME) for all systems supported by INS. Tier III provides third echelon support for network IA devices to all units MCEN wide and provides escalated technical support to Tier II technicians. In conjunction with the Plans and Engineering team, Tier III also provides planning for MCEN IA boundaries for the installation and configuration of all IA network devices located throughout the MCEN, acting as a two-way conduit by consulting with and providing technical guidance to other MCNSOC sections regarding the testing, planning, and implementation of new network IA devices, as well as facilitating the transition of new capabilities to operations when appropriate. Tier III SME's also assist with the review of external or development of internal policies and plans related to MCEN operations in order to ensure standardization and compliance with NetOps requirements throughout the Marine Corps.

The Contractor shall attend weekly Tier III section meetings with Government staff to provide verbal and written updates related to Tier III tasks; problems they have encountered in the past week; and plans for the coming week task completion. The Contractor shall document these Tier III issues and plans in a Tier III INS Weekly Status Report (CDRL A00E) as defined in the INS Desktop procedures.

For all items under this subtask (C.4.3.3.1), the Contractor shall provide 24x7x365 global support at MCNOSC Quantico, Virginia.

C.4.3.3.1.1 INS – OPERATIONS AND MAINTENANCE SUPPORT TIER III

The Contractor shall provide the following Tier III Operations and Maintenance support:

- Operate and maintain the network management and information architecture.
- **Provide 24x7x365 onsite operational support to the MCEN.**
- Migrate users from the legacy networks.
- Maintain systems on-site in accordance with the original equipment manufacturers (OEM) recommended engineering and maintenance practices.
- Perform preventive maintenance, during non-core hours on the system including scheduled preventive maintenance such as periodic tests, inspections, and all other preventive maintenance services/practices recommended by the OEM and as specified in MCNOSC SOPs.
- Perform maintenance after notification that equipment is inoperative and or malfunctioning.
- Provide service personnel trained and certified by the respective OEMs sufficient to ensure system performance and compliance with the maintenance requirements outlined herein.
- Ensure all equipment is maintained in accordance with Original Equipment Manufacturer (OEM) guidelines, MCNOSC SOPs and Local SOPs.

C.4.3.3.1.2 INS – DOMAIN NAME SYSTEM (DNS) SUPPORT TIER III

The Contractor shall provide Tier III DNS support. The DNS environment consists of UNIX and LINUX operating systems, which support the BIND DNS.

The Contractor shall:

- Configure DNS within MCNOSC IA suites.
- Function with BIND DNS including adding, deleting, and changing DNS records, securing DNS configurations based on Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIG) guidance, configuring logging, troubleshooting, and DNS Security (DNSSec) incidents.

C.4.3.3.1.3 INS – UNIX AND LINUX SUPPORT TIER III

The Contractor shall provide Tier III support for the UNIX and LINUX operating systems.

The Contractor shall:

- Configure UNIX and LINUX systems within MCNOSC IA suites.
- Administer UNIX and LINUX including adding, deleting and changing user accounts, securing UNIX/LINUX configurations in accordance with DISA STIGs, configuring system logging (SYSLOG), troubleshooting, and networking.
- Configure, maintain, and operate the Red Had Enterprise LINUX (RHEL) Satellite server which provides centralized patching, provisioning, and configuration capabilities.

C.4.3.3.1.4 INS – NETWORK ROUTER & SWITCH SUPPORT TIER III

The Contractor shall provide Network & Router Switch Support. The environment consists of Cisco, Brocade, Ericson, and Juniper routers and switches.

The Contractor shall:

- Configure router systems within MCEN IA boundary suites.

- Configure Switch systems within IA suites.
- Provide services that include Switch operation, configuration, and maintenance including Spanning Tree Protocol (STP), Virtual Local Area Networks (VLAN), ATM, QoS, and layers 1 and 2 of the OSI networking model.
- Provide services that include Router operation, configuration, and maintenance including dynamic routing protocols (RIPv2, EIGRP, OSPF, IS-IS, BGP, static, PBR), securing Router configurations in accordance with DISA STIGs, configuring system logging (SYSLOG), troubleshooting, Quality of Service (QoS), Access control lists, Virtual Routing and Forwarding (VRF), Multi-Protocol Label Switching (MPLS), Asynchronous Transfer Mode (ATM), and layers 1, 2, and 3 of the Open Systems Interconnect (OSI) networking model.

C.4.3.3.1.5 INS – WAN OPTIMIZATION SUPPORT TIER III
The Contractor shall provide Tier III WAN Optimization Support. The WAN environment is currently supported by Riverbed technology and F5 Load Balancers.

The Contractor shall:
- Configure WAN Optimization systems within MCNOSC IA suites.
- Provide WAN Optimization device operations, configuration, and maintenance of layers 1, 2, and 3 of the OSI networking model.

C.4.3.3.1.6 INS – WEB CONTENT FILTERING SUPPORT TIER III
The Contractor shall provide Web Content Filtering support. The environment is supported by BlueCoat Web Content Filtering devices.

The Contractor shall:
- Configure the Web Content Filter systems within the MCEN IA boundary suites.
- Provide services that include Web Content Filtering device operation, configuration, and maintenance.

C.4.3.3.1.7 INS – FIREWALL SUPPORT TIER III
The Contractor shall provide Tier III Firewall support. The current Firewall technologies to be supported include FortiNet FortiGate, Juniper NetScreen, ISG and SSG, Acme Packet and McAfee Sidewinder Firewalls.

The Contractor shall:
- Configure Firewall systems within MCNOSC IA suites.
- Provide Firewall operations and maintenance including adding, deleting and changing user accounts, securing Firewall configurations in accordance with DISA STIGs, configuring and troubleshooting IP Security (IPSec) and Secure Sockets Layer (SSL) Virtual Private Network (VPN) connections, troubleshooting overall firewall performance and configuration issues, and networking.

C.4.3.3.2 INS – UNIFIED COMMUNICATIONS (UC) SUPPORT
For all items under this subtask, the Contractor shall provide 8x5x52 (Federal business days) global support on site at MCNOSC Quantico, Virginia. The INS Unified

Communications Section provides Tiers I - III support and is responsible for maintaining end-to-end converged IP communication services across the Marine Corps Enterprise Network. The INS UC section implements unified communication and collaboration technologies on the unclassified and classified networks for the Marine Corps while managing effective and efficient technological insertions to achieve IP convergence that is secure and interoperable.

The Contractor is responsible for participating in weekly UC section meetings and providing verbal and written updates related to their UC tasks; problems they have encountered in the past week; and their plans for the upcoming week. The contactor shall provide a weekly UC Status Report (CDRL A00F), as detailed in UC SOPs, documenting UC incidents and meeting outcomes. The Contractor shall conduct Incident Queue Management and ensure that tickets are disseminated in accordance with skill set and MCNOSC Desktop Procedure D03-502.

C.4.3.3.2.1 NETWORK ARCHITECTURE SUPPORT UC
The Contractor shall provide UC network architecture support to operate and maintain the unified communication's enterprise voice and video architecture.

The Contractor shall:

- Conduct Change, Incident, Service Request, Problem, Configuration, and Asset Management per MCNOSC SOPs in order to provide technical end user and core service support. Change Incident and Service Request Management constitutes primary effort and requires the ability to establish and maintain constructive, positive relationships with representatives of Marine Corps Post, Bases and Stations; Defense Information's Systems Agency, MCNOSC Personnel and other contracted staff supporting Marine Corps Network Operations.
- Conduct and document monthly UC Network Architecture Reviews (CDRL A00G), as detailed in UC SOPs, of configurations and settings in order to identify security vulnerabilities, security incidents and conduct appropriate actions to report identified issues and recommend corrective action to the UC Government TPOC.
- Provide network documentation to support MCEN accreditation, auditing and operations per DoD 8510.01 and MCNOSC SOPs (CDRL A00C).
- Review and identify network traffic statistics, equipment, and configurations to provide utilization, capacity, optimization and security reports.
- Conduct onsite survey's in order to identify requirements to facilitate the installation or decommission of equipment and systems.
- Conduct installation and initial connection of equipment and systems locally and remotely.
- Perform preventive maintenance, during non-core hours on the system including scheduled preventive maintenance such as periodic tests, inspections, and all other preventive maintenance services/practices recommended by the OEM and as specified in MCNOSC SOPs.

C.4.3.3.2.2 COMMUNICATIONS AND CAPABILITIES ONSITE SUPPORT UC
The Contractor shall provide direct onsite and regional UC support to major Marine Corps Installations and Commands while maintaining global UC operation support for Critical and High incidents.

C.4.3.3.2.3 VOICE OVER INTERNET PROTOCOL (VOIP) SUPPORT UC

The Contractor shall provide secure VoIP networks, Session Initiation Protocol (SIP), and Skinny Call Control Protocol (SCCP), H.323 protocols. The technologies supporting VoIP support include Windows Server and LINUX operating systems.

The Contractor shall:

- Support the Unified Communications architecture including adding, deleting and changing end instruments, implementing complex call routing schemes, securing VoIP configurations (also SIPRnet) IAW Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIG), configuring logging, firewall traversal, and troubleshooting.
- Configure VoIP within MCNOSC control.

C.4.3.3.2.4 VIDEO TELECONFERENCING (VTC) SUPPORT UC

The Contractor shall provide VTC support including adding, deleting, and changing endpoints, gatekeeper and gateway functionality, securing end instrument configurations in accordance with DISA STIGs, configuring system logging (SYSLOG), troubleshooting, and networking/firewall traversal as well as with the SIP, H.320, and H.323 protocols. The environment consists of Windows Server Operating system and videoconferencing servers.

The Contractor shall:

- Configure, maintain, and operate the videoconferencing servers which provide centralized patching, provisioning, and configuration capabilities of all MCEN VTC endpoints.
- Coordinate with other defense and intelligence agencies to develop and deploy QoS policies in accordance with DISA, HQMC and MCNOSC policies. Configure all Enterprise VTC System within MCNOSC.

C.4.3.3.2.5 QUALITY OF SERVICE (QOS) SUPPORT UC

The Contractor shall provide QoS in support of the MCEN environment. The Contractor shall be responsible for implementation and management of QoS strategies and policies in accordance with SOPs.

The Contractor shall:

- Implement QoS strategies in the LAN and WAN environment to include both strategic and tactical networks
- Work with other defense & intelligence agencies to develop and deploy QoS policies in accordance with DISA, HQMC and MCNOSC policies.
- Provide technical advice and solutions on the configuration of network QoS across the MCEN.

C.4.4 LOCAL IT COMMUNICATIONS SUPPORT

The mission of the Communications Branch is to provide advanced, reliable and secure communications, knowledge management, information systems support (voice, video and data)

and data center management for the MCNOSC Commander and staff in order to enable their global Network Operations mission of operating and defending the MCEN.

The Communications Branch provides 8x5x52 (Federal business days) on site desktop and network support to four buildings on and off base in the local Quantico, VA.

The Communications Branch currently supports approximately 1200 users, and the ancillary devices to support them to include workstations, printers, telephones, Blackberries, servers, switches and Laptops. The average amount of trouble tickets handled by the branch is approximately 1,032 per month at the Quantico, VA location. The Contractor shall perform onsite at the designated Communication Branch locations in Quantico, VA. Travel may be required for the contracted support to assist in Continuity of Operations Plans (COOP) and other exercises at the secondary site, Camp Pendleton, and the Regional Network Operations and Security Centers (RNOSC).

Local IT Communications Core Technologies
Microsoft Exchange, Microsoft Windows Server(2003,2008), Microsoft Group Policy, Active Directory
Microsoft Desktop OS (windows 7), Red Hat Linux(preferred but not required), Windows Remote Desktop Protocol
VMWare ESX, NAS/SAN
Data Center, Telecommunications
BlackBerry, Cell phones and Aircards
Cisco, Juniper, Brocade
IBM Tivoli End point Manager (BigFix), SCCM and Windows Deployment Services, Windows System Update Services
BMC Remedy Incident Management
Retina/Hercules/ACAS/HBSS

The Contractor shall maintain a duty roster for emergency on-call support afterhours support for all tasks under C.4.4. The Contractor shall provide weekly Status Reports (CDRL A00N) to the Communications Branch staff regarding incidents, trends, and other technical issues related to desktop support.

For all subtasks under Task 4, refer to the incident response times required in section C.5.

C.4.4.1 LOCAL IT, INFORMATION ASSURANCE AND NETWORK SUPPORT

The Contractor shall provide Local IT, Information Assurance and Network Support services on three different Networks (NIPR, SIPR and JWICS) for desktop computers, audio-visual, video teleconferences, voice over IP, applications, and related technologies. The Contractor's support includes specifications, installation and testing of computer systems and peripherals within the Information Technology Infrastructure Library (ITIL) version 3 framework established guidelines. The Contractor may require a JWICS account and act as a liaison with Marine Corps Intelligence Activity (MCIA) network support.

The Local IT support will assist MCNOSC with desktop support for Joint Worldwide Intelligence Communications System (JWICS) users and act as an interface with Marine Corps Base Quantico G-6, Marine Corps Cyberspace Command (MARFORCYBER) G-6, Marine Corps Intelligence Activity (MCIA) Chief Information Officer (CIO), and Marine Corps Information Operations Center (MCIOC) S-6 on the communication plan and requirements in reference to the JWICS network (circuits, IP requirements, equipment, software, maintenance, costs).

The environment consists of Microsoft Windows and Office applications as well as other commercial-off-the-shelf applications such as, but not limited to, Adobe Acrobat, Internet Explorer, and Oracle Java plug-ins to provide Local IT Support.

The Contractor shall assist in providing the following Local IT Support services on three different Networks (NIPR, SIPR and JWICS):

- **Provide 8x5x52 (Federal business days) on site Local IT Support** to approximately 1200 global users on the Marine Corps Network and Security Center's local area network for any desktop related problems, to include, but not limited to installation of software and service requests for assets located on the unclassified and classified network.
- Develop and implement a process through which incidents are controlled, this includes problem recognition, research, isolation, resolution, and follow-up steps as defined in the ITIL version 3 framework established guidelines for the Information Technology Service Management (ITSM) discipline for managing information technology (IT) systems.
- Identify, research, and resolve technical problems as related to the user workstations, software and other related user equipment, such as BlackBerries.
- Respond to service requests via Remedy, telephone calls, email, and direct personnel requests for technical support.
- Document, track, and monitor problems to ensure a timely resolution as defined in the ITIL version 3 framework established Guidelines for the Information Technology Service Management (ITSM) discipline for managing information technology (IT) systems, and in accordance with required response times.
- Provide Tier II support to end users for either PC, server, or mainframe applications or hardware.
- Interact with network services, software systems engineering, and applications development to restore service and identify and correct core problem.
- Recommend systems modifications to reduce user problems.
- Support up to 100 global users of the JWICS.
- Interact with Marine Corps Intelligence Activity (MCIA) network services, software systems engineering, and applications development to restore service and identify and correct core problem.
- Perform weekly information assurance scans utilizing Retina or ACAS to check for IAVA compliance (CDRL A00L).
- Remediate any findings identified by the information assurance scans.

The Contractor shall provide Network Administration support for all branded switches (CISCO, Juniper) to include creating virtual local area networks (VLANs), securing port configuration,

managing the configuration files; maintaining the network's integrity including installing new network switch infrastructure, troubleshooting and resolving network issues, as well as developing, applying and enforcing the procedures and policies for use of the Local Area Network. The Contractor shall perform Data Center Management responsibilities and coordination with Enterprise Data Center Manager. The Contractor shall support Information Assurance responsibilities by scanning and remediation for workstations, switches and servers within the Communications Branch area of responsibility. The Contractor is responsible for imaging machines with the latest technologies deployed on the MCEN. The Contractor is responsible for updating Certification and Accreditation (C&A) packages to maintain Authority to Operate (ATO) on the Marine Corps Enterprise Networks (MCEN).

The Contractor shall assist in providing the following Network Administration support:

- Compile, record, and report network operations and maintenance. Troubleshoot network performance issues. Analyzes network traffic and provides capacity planning solutions.
- Monitor and respond to complex technical control facility hardware and network switch operating systems software issues such as misconfigurations and upgrades. Interface with network switch vendors support service groups to ensure proper escalation during outages or periods of degraded system performance.
- Assist in managing the testing, installation, and support of network communications, including LAN/BAN systems.
- Perform Analysis of Alternatives to recommend solutions for network administration support.
- Provide quality assurance review and the evaluation of new and existing software products.
- Provide assistance and oversight for all information systems operations activities, including computer and telecommunications/communications operations, data entry, data control, LAN/BAN administration and operations support, operating systems programming, system security policy procedures, and web strategy and operations.
- Monitor and respond to hardware, software, and network problems.
- Maintain and test network file servers and network printers.
- Provide testing and analysis of all elements of the network facilities (including power, software, communications machinery, lines, modems, and terminals).
- Utilize software and hardware tools and identify and diagnose complex problems and factors affecting network performance.
- Troubleshoot network systems when necessary and makes improvements to the network.
- Manage all of the Communications Branch controlled telecom and server areas.
- Provide Cable and Infrastructure Management, to include:

    - Managing port assignments for network provisioning devices.
    - Providing insight into the configuration and inter-relationship of all multiplexed network devices and cable plant components supporting a provisioned service.
    - Providing a flexible and extendable method to document key management, maintenance and warranty parameters specific to any network device (e.g. network switches, PBX, wireless hubs, etc.)

- Tracking installation and certification parameters for copper, coaxial and fiber optic cable plants
- Identify the installed equipment and cable terminations at various distribution frames (e.g. main, building, intermediate and local telecommunication closets).

Performance Standards and Acceptable Quality Level for Task 4: See attached PRS below.

C.4.5 PROJECT IMPLEMENTATION SUPPORT

Project Implementation is the transition of responsibility of a new or upgraded system or service, from engineering design and development into operational implementation and/or the decommissioning of any system or service from operations. From time to time, the Contractor will be required to staff a short to long term technical project team with the capability to support a specific transition project. Project Implementation Support projects may include upgrading Enterprise Services hardware and software necessary to provide services to the end users, such as routers, switches, firewalls, servers (electronic mail, utility, reporting, scanning, etc.), Information Assurance, and Storage Area Network (SAN) data storage devices. The Enterprise Services upgrade activities include participating in resolving any issues that arise during staging, installation testing, and integration. Ensuring proper operation of all installed equipment is also critical. Ensuring consistency between what was designed and what is actually installed and documented is an expected quality control check.

The established Project Implementation Support team is required to maintain a thorough knowledge of the appropriate MCNOSC Standard Operating Procedures (SOPs), tactics, techniques and procedures (TTPs), and current operational capabilities used in the relative day-to-day Enterprise Services operations. The Contractor shall manage both simple and complex processes of the Enterprise Services environment using the current Standard Operating Procedures (SOPs) and the tactics, techniques and procedures (TTPs) that describe the execution of all facets of operating and sustaining Enterprise Services. The Contractor shall be responsible for developing, reviewing, updating, improving, and documenting current and new Enterprise Services SOPs and TTPs. In addition, Enterprise Services lines of effort require a clear understanding of specific technologies, SOPs, and TTPs. Where a specific Enterprise Services line of effort requires qualification evaluations for new personnel, the Contractor shall develop, review, update, improve, and document current and new billet qualification evaluations as may be directed by the government.

The Contractor shall monitor process activity, analyze SOP applicability, and generate reports to facilitate process improvement. The Contractor shall be responsible for real-time changes or additions to process flows, roles, and forms and the ability to quickly and easily add new processes without impacting daily operations. **During performance of this task, the Contractor shall provide this support onsite 8x5x52 (Federal business days) from MCNOSC Quantico, VA location.**

Performance Standards and Acceptable Quality Level for Task 5: See attached PRS below.

C.4.6 AFTER HOURS SUPPORT

On occasion the MCEN suffers periods of severe network incidents, system and network outages, network attacks, natural disasters, other operational shortcomings, or planned system and network upgrades that require operations and disaster recovery actions beyond the capacity of normal staffing levels. The Contractor shall provide a duty roster for personnel able to immediately respond to these types of incidents. Roster shall exclude task areas that require24x7x365 support/ Duty roster should include individuals that have the ability to provide afterhours capability on short notice (within 2 hours) for the tasks/subtasks specified in this PWS sections C.4.2, C.4.3, and C.4.4.

C.5. ADDITIONAL SUPPORTING INFORMATION

C.5.1 PROJECT MANAGEMENT PLAN REVIEW CHECKLIST

Below are excerpts from the SSCPAC PMP Checklist to assist in PMP Development:

Project Management Plan Review Checklist

Last Update: 2 June 2011

Project Name:	**Review Date:**
IPT Lead:	**Reviewer:**

Purpose: To verify and validate that the Project Management Plan (PMP) and its supporting plans is structured to deliver an acceptable product/service within cost, schedule, scope, and management processes.

Instructions: This review checklist is to be used as a content guide during review of the PMP. It is not intended to be a complete list of all questions to consider, but rather should be used as a starting point. Issues, defects or action items that are uncovered during the review must be documented and communicated back to the PMP owner.

Question #	Checklist Item/Question	Y/N/NA	Notes
	Introduction		
1	Have all revelant guidance documents been referenced in the plan?		
	Project Background		
2	Have the project boundaries and parameters been described in detail to form a clear understanding of the scope?		
3	If applicable, have the appropriate funding sources been identified or described?		
4	Have the project's objectives been clearly described?		
5	Have the assumptions and constraints been documented within the		
6	Are the mechanisms for negotiating and managing project commitments described?		
7	Have the facilities, environment, equipment, technology, processes and support tools required for the project been identified?		

Question #	Checklist Item/Question	Y/N/NA	Notes
8	Is the re-planning process and associated checkpoints adequately described in the plan?		
	Life-cycle		
9	Has a project life-cycle been identified?		
10	Is the project life-cycle clearly defined or referenced in the plan, including definition of all phases?		
	Staffing Plan		
11	Have the required knowledge domains and skillsets required for the project been identfied?		
12	If applicable, does the staffing plan address recognition and rewards, compliance, and safety?		
13	Has a functional organizational chart been included or referenced within the plan?		
14	defined?		
15	If applicable, has the plan for acquiring resources and personnel been defined?		
16	Have the project training requirements been defined?		
	Stakeholder Involvement		
17	Have all project stakeholders been identified, including contact information?		
18	Has the stakeholder management approach been defined?		
19	Does the stakeholder management approach consider the following: identification of how the stakeholder impacts the project, stakeholder's level of participation and identification of stakeholder groups?		
20	Has a process or venue for escalating concerns to stakeholders in regard to risks, issues and schedules been identified?		
	Communication Plan		
21	Has a communication approach been defined that addresses project stakeholder information needs?		
22	Does the communication plan identify and describe the mechanisms for communicating content, including audience, purpose, frequency, and type(s)/method(s) ?		
	Project Management		

Question #	Checklist Item/Question	Y/N/NA	Notes
23	Have the high level project management proceses been described?		
24	Have the estimating processes, procedures and techniques been described or referenced?		
25	Have the triggers for re-estimation been identified?		
26	Have all of the work products and/or services being delivered by the project been listed or referenced?		
27	Has the project schedule been clearly defined or referenced?		
28	Does the schedule address the following: list of work activities, milestones, time-sequencing, resource estimates, duration estimates, and resource assignments?		
29	Is there a reference to the budget's storage location?		
	Quality Management		
30	Have the quality assurance processes been described?		
31	Have the methods been described that will be used to provide configuration/data item identification, control, status accounting, evaluation and release management?		
32	Has the verification and validation plan for the project been defined, including scope, tools, techniques and responsibilities for the verification and validation work activities?		
	Risk Management		
33	Have the risk management processes been described, including the methodology, timing, risk categroies, probability, impact and reporting formats?		
	Measurement and Analysis		
34	Have the methods, tools and techniques for collecting and retaining project metrics been defined?		
35	Does the measurement and analysis plan address metrics collection, frequency of collection, data storage and methods for validating, analyzing and reporting metrics?		
	Monitoring and Control		
36	Have the mechanisms for monitoring and controlling the schedule, budget, resources and quality of work products been defined?		
37	Are all elements of the monitoring and control plan consistent with the organization's standards, policies and procedures for project control?		

Question #	Checklist Item/Question	Y/N/NA	Notes
38	Are project reviews clearly identified?		

C.5.2 SERVICE TARGET REQUIREMENTS BY URGENCY LEVEL

The timeliness of responses and resolutions below are determined by comparing the urgency and impact of an incident as defined in the tables below. The inputs are then auto calculated into a priority designation using the Remedy system.

- Timeliness of Responses and Resolution date:

  Target metrics for Incidents, Work Orders, and Service Requests:

Severity	Critical	High	Medium	Low
Assignment to technician / initialed response	10 Minutes	30 Minutes	60 Minutes	60 Minutes
Updates	90 Minutes	12 Hours	72 Hours	7 Days
Updates when at "Pending" Status	90 Minutes	24 Hours	7 Days, 4 Hours	14 Days
Resolution	8 hours	24 Hours	5 Days	10 Days

- Resolution time exclude times when the record is in a "Pending" status.

C.5.3 INCIDENT IMPACT DETERMINATION

Table: MCNOSC Incident/Event Impact Levels

Impact Levels	*Affected MCEN Customer*	*Affected System/Service*	*BC Discretion Guidance*
Extensive/Widespread	Multiple Bases/Posts/Sites	MAC I System/Service -Or- MAC II System/Service degraded >50%	Capabilities vital to mission effectiveness or operational readiness of deployed or contingency forces are impacted
Significant/Large	An Entire Base/Post/Site	MAC II System/Service degraded <50% -Or- MAC III System/Service degraded >50%	Capabilities vital to mission effectiveness or operational readiness of deployed or contingency forces are impacted

Moderate/Limited	Multiple Customers	MAC III System/Service degraded <50%	N/A
Minor/Localized	An Individual Customer	N/A	N/A

MAC 1 These systems handle information that is determined to be vital to the operational readiness of mission effectiveness of deployed and contingency forces in terms of both content and timeliness.
MAC 2 These systems handle information that is important to the support of deployed and contingency forces.
MAC 3 These systems handle information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term.

C.5.4 INCIDENT URGENCY DETERMINATION

Urgency is a measure of how long it will be until the Incident will have an impact on the affected customer(s). When evaluating and selecting urgency, consider the customer's required time to resolution, the availability of a work-around, VIP status, and risk. The four categories are defined in the table below. The category will be annotated in the Urgency Field of the record.

Table: MCNOSC Urgency Categories

Urgency Categories	Required time to resolve	Work-around Availability	Risk	Customer
Critical	Immediate resolution or fulfillment of Service Request is required	Work-around not available and the need to achieve desired action is immediate	Risk is High that Impact will increase significantly if immediate resolution is not achieved	Customer Billet or mission requires immediate resolution or fulfillment
High	Additional resources should be allocated to facilitate timely resolution or fulfillment above routine work	Work-around not available but work can be temporarily shifted to other activities	Plausible Risk that Impact will increase if resolution is not achieved	Routine work
Medium	Work to be accomplished is routine in nature	Work-around exists but productivity affected	System or service available, but degraded	Routine work
Low	Resolution or Service Request fulfillment is	Work-around exists	Productivity effect is minimal or non-	Routine work

Urgency Categories	Required time to resolve	Work-around Availability	Risk	Customer
	required, but at a low urgency		existent	

C.5.5 INCIDENT PRIORITY DESIGNATION

The Incident Priority and Weight are auto-calculated and auto-populated by the Remedy system in accordance with the table below, based on selected values for Impact and Urgency. Weight can be used to distribute activities more efficiently across the command's workforce.

Table: MCNOSC Priority Table

URGENCY	IMPACT				
		Extensive / Widespread 9	**Significant / Larger 5**	**Moderate / Limited 3**	**Minor / Localized 0**
	Critical 20	**Critical 29**	**Critical 25**	**High 23**	**High 20**
	High 15	**Critical 24**	**High 20**	**High 18**	**Medium 15**
	Medium 10	**High 19**	**Medium 15**	**Medium 13**	**Medium 10**
	Low 0	**Low 9**	**Low 5**	**Low 3**	**Low 0**

C.5.6 ESTIMATED LEVEL OF EFFORT, CLEARANCE REQUIREMENTS, LOCATIONS, & SHIFTS

The following tables illustrate the estimated labor effort per scope area, including locations, shifts, and required clearances.

Clearances, Hours & Locations by Task.

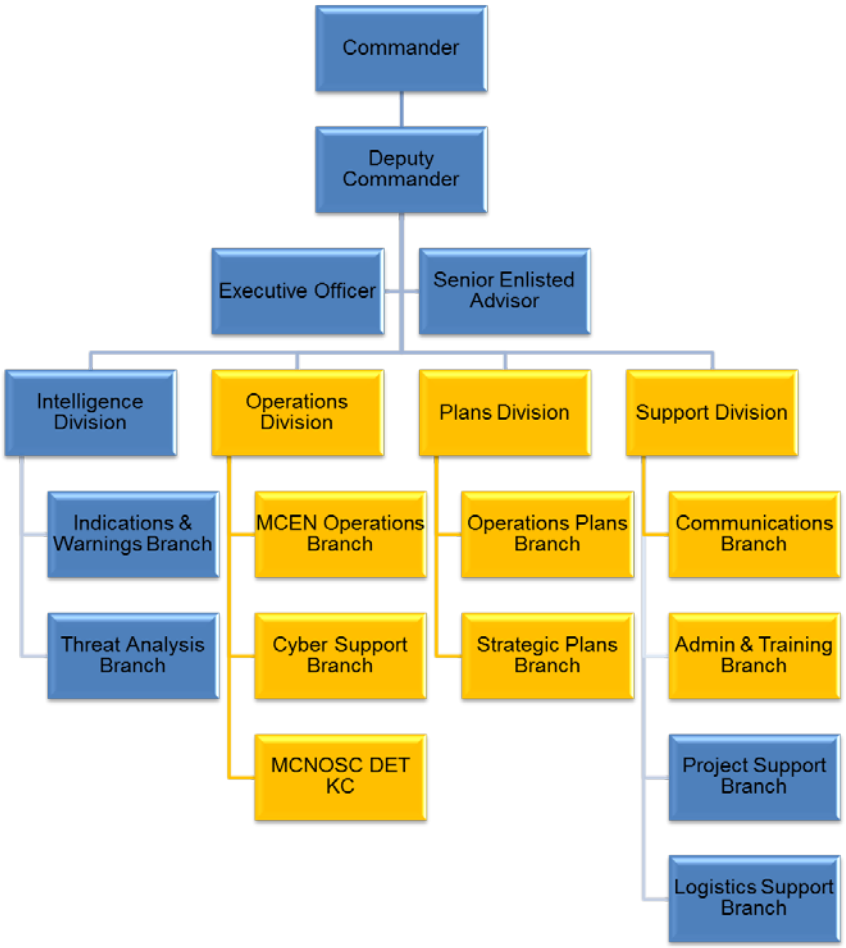
Resources are expressed as Full-Time-Equivalent (FTE) requirements, which are expected to be satisfied with full-time team members assigned to the overall task. An FTE for the purposes of this task order equates 1920 direct productive labor hours per year. The FTEs expressed below should not be construed as absolute values per labor category, but rather the total level of effort the Government expects in terms of contractor support.

Task Area	Alliant Labor Category	MCNOSC Functional Role or Labor Category	Clearance	Location	Shift	Man year hours	Personnel	Total Hours
Task C.4.1: Program Management								
PROGRAM MANAGEMENT	Program Manager	PROGRAM MANAGER	TOP SECRET	Quantico	8hrs/5 days/w	1920	1.0	1920
Task C.4.2: Operations Division & Cyber Support Branch								
Operations	Information Assurance/Security Specialist (Journeyman)	ACAS Vulnerability Analyst	SECRET	Quantico	8hrs/5 days/w	1920	2	3840
Operations	Information Assurance/Security Specialist (Journeyman)	ACAS Vulnerability Administrator	SECRET	Quantico	8hrs/5 days/w	1920	2	3840
CSB	Applications Systems Analyst (Master)	NetCop - (BMC Tools Admin and Architecture Support)	SECRET	Quantico	8hrs/5 days/w	1920	2.0	3840
CSB	Applications Systems Analyst (Senior)	NetCop - (BMC Tools Admin and Architecture Support)	SECRET	Quantico	8hrs/5 days/w	1920	1.0	1920
CSB	Applications Systems Analyst (Master)	NetCop - (Event Management Tools)	SECRET	Quantico	8hrs/5 days/w	1920	1.0	1920
CSB	Applications Systems Analyst (Senior)	NetCop - (Event Management Tools)	SECRET	Quantico	8hrs/5 days/w	1920	1.0	1920
CSB	Applications Developer (Senior)	NetCop - (Software Developer)	SECRET	Quantico	8hrs/5 days/w	1920	2.0	3840
CSB	Web Designer	NetCop - (WEB DESIGNER)	SECRET	Quantico	8hrs/5 days/w	1920	1.0	1920
CSB	Configuration Management Specialist (Journeyman)	Configuration Management Specialist	SECRET	Quantico	8hrs/5 days/w	1920	2.0	3840
Total							**14**	**26,880**
Task C.4.3: MCEN Operations Branch								
MCEN OPERATIONS SUPPPORT	Applications Developer (Senior)	EDM - SR. WEB DEVELOPER	TS/SCI	Quantico	8hrs/5 days/w	1920	1.0	1920
MCEN OPERATIONS SUPPPORT	Voice/Data Communications Engineer (Senior)	INS - NETWORK ENGINEER III (Voice over IP)	TS/SCI	Quantico	8hrs/5 days/w	1920	1.0	1920
MCEN OPERATIONS SUPPPORT	Voice/Data Communications Engineer (Senior)	INS - NETWORK ENGINEER III (Enterprise VTC)	TS/SCI	Quantico	8hrs/5 days/w	1920	1.0	1920
MCEN OPERATIONS SUPPPORT	Network Specialist (Master)	INS - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (DOMAIN NAME SYSTEM)	SECRET	Quantico	8hrs/5 days/w	1920	1.0	1920
MCEN OPERATIONS SUPPPORT	Network Specialist (Master)	INS - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (ROUTING AND SWITCHING)	TS/SCI	Quantico	8hrs/5 days/w	1920	1.0	1920
MCEN OPERATIONS SUPPPORT	Applications Developer (Master)	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (ACTIVE DIRECTORY)	TS/SCI	Quantico	8hrs/5 days/w	1920	1	1920
MCEN OPERATIONS SUPPPORT	Applications Developer (Senior)	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (ACTIVE DIRECTORY)	TS/SCI	Quantico	8hrs/5 days/w	1920	3	5760
MCEN OPERATIONS SUPPPORT	Applications Developer (Senior)	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (THREAT MANAGEMENT GATEWAY)/F5	TS/SCI	Quantico	8hrs/5 days/w k	1920	2	3840
MCEN OPERATIONS SUPPPORT	Applications Developer (Master)	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (MS EXCHANGE)	TS/SCI	Quantico	8hrs/5 days/w	1920	2	3840
MCEN OPERATIONS SUPPPORT	Applications Developer (Senior)	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (MS EXCHANGE)	TS/SCI	Quantico	8hrs/5 days/w	1920	4	7680

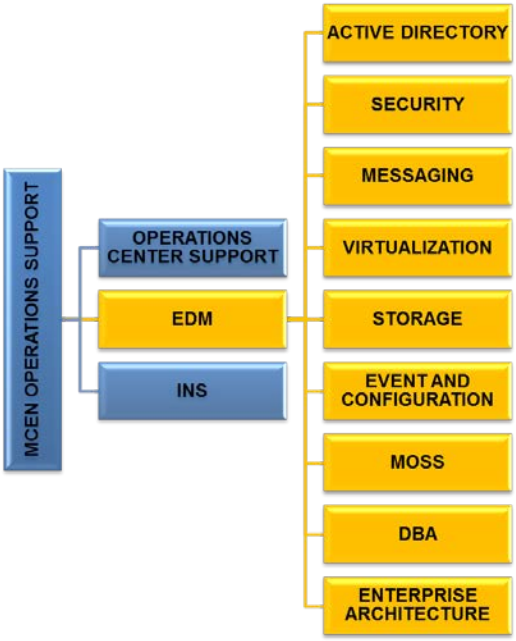
Task Area	Alliant Labor Category	MCNOSC Functional Role or Labor Category	Clearance	Location	Shift	Man year hours	Personnel	Total Hours
MCEN OPERATIONS SUPPPORT	Applications Developer (Master)	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (VIRTUALIZATION)	TS/SCI	Quantico	8hrs/5 days/w	1920	1	1920
MCEN OPERATIONS SUPPPORT	Applications Developer (Senior)	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (VIRTUALIZATION)	TS/SCI	Quantico	8hrs/5 days/w	1920	3	5760
MCEN OPERATIONS SUPPPORT	Applications Developer (Master)	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (STORAGE AREA NETWORKING)	TS/SCI	Quantico	8hrs/5 days/w	1920	1	1920
MCEN OPERATIONS SUPPPORT	Applications Developer (Senior)	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (STORAGE AREA NETWORKING)	TS/SCI	Quantico	8hrs/5 days/w	1920	3	5760
MCEN OPERATIONS SUPPPORT	Applications Developer (Master)	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (CONFIGURATION MANAGEMENT)	TS/SCI	Quantico	8hrs/5 days/w	1920	1	1920
MCEN OPERATIONS SUPPPORT	Applications Developer (Senior)	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (CONFIGURATION MANAGEMENT)	TS/SCI	Quantico	8hrs/5 days/w	1920	2	3840
MCEN OPERATIONS SUPPPORT	Disaster Recovery Specialist (Senior)	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (CONFIGURATION MANAGEMENT)	TS/SCI	Quantico	8hrs/5 days/w	1920	3	5760
MCEN OPERATIONS SUPPPORT	Database Specialist (Master)	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (DATABASE ADMINISTRATION)	TS/SCI	Quantico	8hrs/5 days/w	1920	2	3840
MCEN OPERATIONS SUPPPORT	Applications Developer (Senior)	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (MS EXCHANGE & ACTIVE DIRECTORY) (24/7)	TS/SCI	Quantico	24/7/365	1920	4	7680
MCEN OPERATIONS SUPPPORT	Data Architect	EDM - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (DATA ARCHITECT)	TS/SCI	Quantico	8hrs/5 days/w	1920	1	1920
MCEN OPERATIONS SUPPPORT	Network Specialist (Master)	INS - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (WAN OPTIMIZATION)	SECRET	Quantico	8hrs/5 days/w	1920	1	1920
MCEN OPERATIONS SUPPPORT	Network Specialist (Master)	INS - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (WEB CONTENT FILTERING)	SECRET	Quantico	8hrs/5 days/w	1920	2	3840
MCEN OPERATIONS SUPPPORT	Network Specialist (Master)	INS - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (FIREWALL)	TS/SCI	Quantico	8hrs/5 days/w	1920	1	1920
MCEN OPERATIONS SUPPPORT	Network Specialist (Master)	INS - SUBJECT MATTER EXPERT (NETWORK ENGINEERING) (ROUTING AND SWITCHING/FIREWALL/VPN - 24X7X365)	TS/SCI	Quantico	24/7/365	1920	5	9600
MCEN OPERATIONS SUPPPORT	Information Assurance/Security Specialist (Senior)	INS - WAN RESOURCE MANAGEMENT (AUDITING/QUALITY ASSURANCE)	SECRET	Quantico	8hrs/5 days/w	1920	2	3840
MCEN OPERATIONS SUPPPORT	Network Specialist (Journeyman)	OPS/CTR - WATCH TEAM SUPPORT (NETWORK SERVICES)(24/7)	TS/SCI	Quantico	24/7/365	1920	4	7680
MCEN OPERATIONS SUPPPORT	Helpdesk Specialist (Journeyman)	OPS/CTR NOC SERVICE DESK (SUBJECT MATTER EXPERT) (SENIOR) (KC)(24/5)	SECRET	Kansas City	24/5	1920	3	5760
MCEN OPERATIONS SUPPPORT	Helpdesk Specialist (Journeyman)	OPS/CTR NOC SERVICE DESK (SUBJECT MATTER EXPERT) (SENIOR) (QUANTICO)(24/5)	SECRET	Quantico	24/5	1920	3	5760
MCEN OPERATIONS SUPPPORT	Quality Assurance Specialist (Entry Level)	OPS/CTR - IT BUSINESS PROCESS QUALITY CONTROL	SECRET	Quantico	8hrs/5 days/w	1920	1	1920
MCEN OPERATIONS SUPPPORT	Research Analyst	OPS/CTR - INCIDENT AND SERVICE MANAGEMENT SUPPORT (24/5)	SECRET	Kansas City	24/5	1920	3	5760
MCEN OPERATIONS SUPPPORT	Configuration Management Specialist (Journeyman)	OPS/CTR - CHANGE/RELEASE AND DEPLOYMENT MANAGEMENT SUPPORT	SECRET	Quantico	8hrs/5 days/w	1920	2	3840
Total							65	124,800
Task C.4.4: LOCAL IT SUPPORT								
LOCAL IT SUPPORT	Network Specialist (Journeyman)	Local IT Support(NIPR,SIPR,JWICS, IA)	TS/SCI	Quantico	8hrs/5 days/w	1920	3.0	5760
LOCAL IT SUPPORT	Information Assurance/Security Specialist (Entry Level)	Information Assurance/Security Specialist	TS/SCI	Quantico	8hrs/5 days/w	1920	2.0	3840
Total							5	9,600
Task Area	Alliant Labor Category	MCNOSC Functional Role or Labor Category	Clearance	Location	Shift	Man year hours	Personnel	Total Hours
Task C.4.5: Project Implementation Team Support								
Task Area	Alliant Labor Category	MCNOSC Labor Category		Location		Man year hours	Personnel	Total Hours
Operations	Network Specialist (Master)	Transition Team (NETWORK ENGINEERING) (Active Directory)	SECRET	Quantico	8hrs/5 days/w	1920	2	3840
Operations	Network Specialist (Master)	Transition Team (NETWORK ENGINEERING) (MS EXCHANGE)	SECRET	Quantico	8hrs/5 days/w	1920	2	3840
Operations	Network Specialist (Master)	Transition Team (VIRTUALIZATION)	SECRET	Quantico	8hrs/5 days/w	1920	2	3840
Operations	Network Specialist (Master)	Transition Team (NETWORK ENGINEERING) (ROUTING AND SWITCHING)	SECRET	Quantico	8hrs/5 days/w	1920	2	3840
Operations	Information Assurance/Security Specialist (Master)	Transition Team (INFORMATION ASSURANCE/SECURITY SPECIALIST)	SECRET	Quantico	8hrs/5 days/w	1920	2.0	3840
Total							10	19,200
C.4.6: After Hours Support								
Various	Various	Various	SECRET	Quantico	Various	1920	3.0	5760
Total							3.0	5760
Grand Total							98	188,160

C.5.7 ORGANIZATION CHARTS

Organization Chart 1



Organization Chart 2



C.6 DELIVERABLES

The Contractor shall deliver all electronic versions by email and removable electronic media, as well as placing in the MCNOSC designated repository. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

a. Text MS Word, Google Docs
b. Spreadsheets MS Excel, Google Sheets
c. Briefings MS PowerPoint, Google Slides
d. Drawings MS Visio, Google Drawings
e. Schedules MS Project, Smartsheet

The following schedule of milestones will be used by the SSCPAC COR to monitor timely progress under this TO. The following abbreviations are used in this schedule:

NLT: No Later Than
TOA: Task Order Award
IAW PMP: In Accordance With Project Management Plan
All references to days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

See attached Contract Deliverables Requirements List (CDRLs, Attachment B) for more information. The Contractor shall deliver the deliverables listed in the following table:

CDRL. #	MILESTONE/ DELIVERABLE	PWSREFERENCE	PLANNED COMPLETION DATE	DATA RIGHTS CLAUSE
	Project Start (PS)		At TOA	N/A
A001	Kick-Off Meeting	C.4.1.1	Within 3 workdays of TOA	N/A
A002	Copy of TO (initial award and all modifications)		Within 10 workdays of award	N/A
A003	Transition-Out Plan – Final	C.4.1	Draft NLT 90 calendar days prior to expiration of the TO, final 45 days prior to expiration of TO.	N/A
A004	Transition-In Plan – Final	C.4.1	3 workdays after the Project Kick-Off Meeting	N/A
A005	Technical Status Meetings	C.4.1	Monthly	N/A

CDRL. #	MILESTONE/ DELIVERABLE	PWSREFERENCE	PLANNED COMPLETION DATE	DATA RIGHTS CLAUSE
A006	Project Management Plan – Final	C.4.1	10 workdays after receipt of Government comments	N/A
A007	Monthly Status Report	C.4.1	10th calendar day of the next month	N/A
A008	Meeting Minutes	C.4.1	Within 24 hours of the scheduled meeting	N/A
A009	Trip Report(s)	C.4.1	Within 10 workdays following completion of each trip	N/A
A00A	EDM Weekly Status Report	C.4.3.2	Weekly	
A00B	EDM SAN Capacity and Performance Report	C.4.3.2	Monthly	
A00C	Design Documentation, Instructions and Procedures	C.4.4	IAW	
A00D	Technical Architecture Findings Report	C.4.3.2	Quarterly	
A00E	Tier III INS Status Report	C.4.3.3	Weekly	
A00F	UC Status Report	C.4.3.3	Weekly	
A00G	UC Network Architecture Report	C.4.3.3	Monthly	
A00H	Watch Team Status Report	C.4.3.1	Weekly	
A00J	Post-Incident Report	C.4.3.1	IAW	
A00K	Service Desk Performance Metrics	C.4.3.1	Weekly and Monthly Reviews	
A00L	IAVA Compliance Report	C.4.4.1	Weekly	
A00M	ACAS Support Documentation	C.4.2.2.	As needed	
A00N	Communications Weekly Status Reports	C.4.4	Weekly	

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-confirming markings in accordance with 252.227-7013.

C.7. TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Joint Travel Regulation (JTR) - prescribed by the GSA, for travel in the contiguous U.S.
b. Federal Travel Regulation (FTR) Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

The Contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR/FTR/DSSR. The invoice shall include the period of performance covered by the invoice, the CLIN number, task area, and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

All cost presentations provided by the Contractor shall also include Overhead charges and General and Administrative charges in accordance with the Contractor’s DCAA cost disclosure statement.

For the purposes of estimating, the following travel is expected under this Task Order:

How Many Trips	From Location	Destination	# of FTEs	Travel Requirements	Duration
2	Quantico, VA	Savannah, GA	1	Flight, Rental Car, and Lodging	3 Days
2	Quantico, VA	Waukegan, IL	1	Flight, Rental Car, Lodging	3 Days
2	Quantico, VA	Wahpeton, ND	1	Flight, Rental Car, Lodging	3 Days
2	Quantico, VA	Texarkana, TX	1	Flight, Rental Car, Lodging	3 Day
2	Quantico, VA	Grand Prairie, TX	1	Flight, Rental Car, Lodging	3 Day
2	Quantico, VA	Yakima, WA	1	Flight, Rental Car, Lodging	3 Days

5	Quantico, VA	Twentynine Palms, CA	1	Flight, Rental Car, Lodging	3 Days
5	Quantico, VA	MCAS Yuma, AZ	1	Flight, Rental Car, Lodging	3 Days
5	Quantico, VA	Barstow, CA	1	Flight, Rental Car, Lodging	3 Days
3	Quantico, VA	Bridgeport, CA	1	Flight, Rental Car, Lodging	3 Days
2	Quantico, VA	Charlotte, NC	1	Rental Car, Lodging	3 Days
2	Quantico, VA	Eastover, SC	1	Rental Car, Lodging	3 Days
5	Quantico, VA	Parris Island, SC	1	Flight, Rental Car, Lodging	2 Days
5	Quantico, VA	Beaufort, SC	1	Rental Car, Lodging	2 Days
5	Quantico, VA	Albany, GA	1	Flight, Rental Car, Lodging	3 Days
3	Quantico, VA	Bahrain	1	Flight, Rental Car, Lodging	5 Days
5	Quantico, VA	Blount Island, FL	1	Flight, Rental Car, Lodging	3 Days
5	Quantico, VA	Tampa, FL	1	Flight, Rental Car, Lodging	3 Days
5	Quantico, VA	Norfolk, VA	1	POV	2 Days
5	Quantico, VA	Wyoming, PA	1	Rental Car, Lodging	3 Days
5	Quantico, VA	Charleston, WV	1	Rental Car, Lodging	3 days
10	Quantico, VA	Kansas City, MO	1	Flight, Rental Car, Lodging	3 Days
3	Kansas City, MO	Quantico, VA	3	Flight, Rental Car, Lodging	3 Days
5	Quantico, VA	Indianapolis, IN	1	Flight, Rental Car, Lodging	3 Days
2	Quantico, VA	Indian Head, MD	1	POV	1
20	Quantico, VA	Washington D.C.	1	POV	1 Day
5	Quantico, VA	Mechanicsburg, PA	1	POV	1 Day

4	Quantico, VA	Stuttgart, Germany	1	Flight, Rental Car, Lodging	5 Days
3	Quantico, VA	MCAS Iwakuni, Japan	1	Flight, Rental Car, Lodging	5 Days
3	Quantico, VA	Seoul, Korea	1	Flight, Rental Car, Lodging	5 Days
3	Quantico, VA	Camp Fuji	1	Flight, Rental Car, Lodging	5 Days

C.8. GENERAL PERSONNEL REQUIREMENTS

C.8.1 INFORMATION ASSURANCE WORKFORCE IMPROVEMENT PROGRAM

The DoD 8570.01-M "Information Assurance Workforce Improvement Program" (dated 24 Jan 2012 or later) established the guidance for personnel requirements conducting Information Assurance (IA) functions. The Contractor must be compliant with the DoD 8570 IA requirement established by MCNOSC (table below) within 180 days of the start of the task order or employee hire, except where specified in section C.4.1.8. In accordance with DFARS clause 252.239-7001 and PGI 239.7102, the Contractor shall submit proof of certifications attained for both key and non-key personnel upon request from the Government.

Task Area	IA 8570 Requirement
Program Management	IAT III
NETCOP – BMC Tools Administration	IAT II
NETCOP – Event Management	IAT II
NETCOP – OPDRS	IAT II
MAINFRAME	IAT II
Ops Center – Watch Team	IAM I
Ops Center – NOC	IAM I
Ops Center – Business Process	IAM II
Ops Center – Incident Management	IAM I
Ops Center – QC	IAM I
Ops Center – Change/Release/Deploy	IAM II
EDM	IAT III
INS	IAT III, IAM III, IASAE II, and CND-IS
INS – UC	IAT III
Local IT Support	IAT II
Operational Transition Support	IAT III or IAM III
ACAS Support	IAT III or IAM II

C.8.2 GUIDANCE FOR TECHNICAL PERSONNEL

The MCNOSC relies on technical subject matter expertise of its Contractor's to support the operations and maintenance of the MCEN. Given the level of technical support that is often required to troubleshoot and execute the technical functions described in the PWS, the Government has established guidance for understanding the technical skills, education and certifications that may be required to support the MCNOSC environment. The Government is in no way prescribing these as personnel requirements rather providing guidance for Contractor personnel to understand the general qualifications for technical personnel. See section C.9SECURITY CLEARANCES below for mandatory clearance requirements.

Task Area	Technical Certification(s) & Education
Enterprise Directory and Messaging	MCM, MCSE, MCITP, VCDX5-DCV, NCIE, ITIL V3 Foundations
Integrated Network Support	RHCE, CCIE, JNCIE, CCNP, Fortinet NSE 5, ITIL V3 Foundations
Local IT Support	MCDST, VCP, Windows OS, Network+, A+, CCNA, JNCIA, ITIL V3 Foundations
Operations Center	BMC ITSM Suite, Sharepoint, HP BSM, UCMDB, OMW, NNMI, HP SiteScope, HP Universal Discovery, HP SHR, HP SHA, HP SHO, HP RUM, MCP, MCSD, BMC Atrium, IBM Mainframe Utility, ITIL V3 Foundations

Note: All training required to meet the minimum personnel qualifications and certifications set forth in the PWS are the responsibility of the contractor to fund and provide. The Contractor may be required to enroll in and receive specialized training provided by the Government beyond the qualifications listed in the PWS at locations to be determined. Tuition, labor, and travel expenses associated with Government requested training are considered allowable expenses under this contract and shall be conducted in accordance with the Joint Travel Regulations (JTR). All anticipated training and travel expenses must be approved in writing by the COR prior to training enrollment.

C.8.3 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key."

a. Program Manager (PM)
b. Enterprise Directory and Messaging (EDM) Technical Lead
c. Integrated Network Support (INS) Technical Lead

d. Operations Center Technical Lead
e. Local IT Support Lead

The Government desires that Key Personnel be assigned for the duration of the TO. The Contractor may propose additional Key Personnel, subject to Government approval, as it pertains to the solution offered. The Government requires that Key Personnel be assigned for the duration of the TO. Proposed replacement of Key Personnel shall be in accordance with paragraph C8.4 of the PWS. If Key Personnel turnover occurs, the contractor shall propose a replacement within three business days. The Government will review proposed Key Personnel replacement and either approve or reject replacement within three business days.

C.8.3.1 PROGRAM MANAGER

It is required that the PM has the following qualifications:

a. Active PMI PMP
b. A minimum of a Bachelor's degree in Management or related Technology field.
c. At least ten years of experience managing a contract/task order of similar size, scope, and complexity to that outlined in this PWS.
d. At least five years' demonstrated experience supporting a C4 environment consisting of similar network applications and systems described in the TOR.
e. Information Assurance Technician (IAT) level III
f. Top Secret (SCI Eligible) Clearance

It is desired that the PM has the following qualifications:

a. ITIL v3 Foundation Certification

C.8.3.2 MASTER APPLICATIONS DEVELOPER (EDM TECHNICAL LEAD)

It is required that the EDM Technical Lead has the following qualifications:

a. At least seven years of demonstrated experience leading senior technicians in a geographically distributed classified network environment.
b. At least five years of experience supporting an Active Directory, Microsoft Exchange, SAN, and Virtualization enterprise level environment.
c. Microsoft Certified Systems Engineer (MCSE)
d. IAT Level III
e. Top Secret (SCI Eligible) Clearance

It is desired that the EDM Technical Lead has the following qualifications:

a. ITIL v3 Foundation Certification
b. Demonstrated experience supporting an enterprise network environment consisting of 200k users
c. Demonstrated experience engineering enterprise NetApp storage solutions
d. Demonstrated experience engineering enterprise VMware solutions
e. Experience working with Microsoft System Center to automate critical tasks.

C.8.3.3 MASTER NETWORK SPECIALIST (INS TECHNICAL LEAD)

It is required that the INS Technical Lead has the following qualifications:

a. At least five years of experience leading senior technicians in a DoD network environment supporting Tier II – Tier III DNS, LINUX, Firewalls, WAN Optimization, and Routing and Switching.

b. IAT level III
c. Top Secret (SCI Eligible) Clearance

It is desired that the INS Technical Lead has the following qualifications:

a. ITIL v3 Foundation Certification

C.8.3.4 HELPDESK SPECIALIST (OPERATIONS CENTER TECHNICAL LEAD)

It is required that the PM has the following qualifications:

a. At least five years of demonstrated experience leading technical personnel in the fields of business process management and/or managing a service desk environment.
b. Information Assurance Manager (IAM) level II
c. Top Secret (SCI Eligible) Clearance

It is desired that the Operations Center Technical Lead has the following qualifications:

a. ITIL v3 Foundation Certification

C.8.3.5 NETWORK SPECIALIST (LOCAL IT SUPPORT LEAD)

It is required that the Local IT Support Lead has the following qualifications:

a. At least five years of demonstrated experience leading senior IT technicians in a local IT network environment.
b. IAT level II
c. Top Secret (SCI Eligible) Clearance

It is desired that the Local IT Support Lead has the following qualifications:

a. ITIL v3 Foundation Certification
b. Microsoft Certified Desktop Support Technician (MCDST)
c. VMWare Certified Professional (VCP)

C.8.4 KEY PERSONNEL SUBSTITUTION

Key Personnel may only be replaced or removed subject to the requirements herein.
The Contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the CO. Prior to utilizing other than personnel specified in proposals in response to a TOR, the Contractor shall notify the Government CO and the COR of the existing TO. This notification shall be no later than *ten* calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.
Substitute personnel qualifications shall be equal to, or greater than, those of the personnel being substituted. If the Government CO and the COR determine that a proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the Contractor may be subject to default action as prescribed

C.9.1 OPERATIONS SECURITY (OPSEC)

OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or Critical Program Information, and therefore all Contractor personnel must practice OPSEC. All work is to be

performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD254.

Applicable documents are as follows OPNAVINST F3300.53C (Series), Navy Antiterrorism Program, National Security Decision Directive 298 (Series), National Operations Security Program (NSDD) 298, DOD 5205.02 (Series), DOD Operations Security (OPSEC) Program, OPNAVINST 3432.1 (Series), DON Operations Security, and SPAWARINST 3432.1 (Series), Operations Security Policy.

C.9.2 INFORMATION ASSURANCE

The Contractor may have access to sensitive (to include privileged and confidential) data, information, and materials of the U.S. Government. These printed and electronic documents are for internal use only and remain the sole property of the U.S. Government. Some of these materials are protected by the Privacy Act of 1974 (AMENDED) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

C.9.3 SECURITY CLEARANCES

Specific personnel supporting this contract have access to the highest network privileges in the USMC. Privileged access allows personnel to make enterprise level changes concerning the network. Therefore, privileged access is limited to personnel with a Top Secret (SCI Access). All personnel with privileged access include:

- All EDM Platform Administrators (C.4.3.2.1, C.4.3.2.2 EDM)
- All Tier III level or higher supporting Active Directory (C.3 Active Directory)
- All JWICS and Network Administration support (C.4.4 Local IT)

See Section C.5: Clearances, Hours, & Locations for detailed clearance requirements by task area.

The Contractor may be required to respond to emerging requirements set forth by the DoD and USMC that change privileged access permissions.

The remaining personnel must possess upon award, at a minimum, an adjudicated Secret clearance.

This acquisition requires all work to be performed at a controlled access facility belonging to the Government. Contractor personnel are required to have a final/interim TS or secret personnel security clearance (PCL), as applicable, in order to have unescorted access within the facility. The Government will not provide escorts or bear additional costs associated with meeting the access requirement. The prime Contractor must have a TS facility clearance (FCL), or higher, as of the closing date of the solicitation in order to support the personnel security clearance requirement. The lengthy process involved in obtaining an FCL, and the possibility of a negative outcome that would render the Contractor unable to perform the contract, could make the agency vulnerable to delays in contract performance.

C.10 Enterprise Contractor Manpower Reporting Application (ECMRA)

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address https://doncmra.nmci.navy.mil.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year

(FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at http://www.ecmra.mil/.

Performance Requirement Summary (PRS)

Performance Objectives, Standards, and AQLs				
OBJECTIVES	**SOW / PWS (PARA)**	**CDRL #**	**EXPECTED STANDARD**	**ACCEPTABLE QUALITY LEVEL (AQL)**
Kick-Off Meeting	C.4.1.1	A001	Meeting includes agenda that covers contract requirements and execution strategy. Agenda items are briefed and all questions answered. Follow-on actions and meeting minutes are recorded.	Presentation is professional and covers the contractor's strategies for executing each awarded task element.
Copy of TO (initial award and all modifications)		A002	Contract includes all awarded conformed documents.	No documents missing. Documents include required signatures.
Transition-Out Plan – Final	C.4.1	A003	Plan is clear, concise, and free of typographical errors. Plan includes sound strategy for transition out of the contract that ensures continuity of operations for the MCNOSC.	Plan contains less than 2% of typographical errors. All operational areas covered in plan.
Transition-In Plan - Final	C.4.1	A004	Plan is clear, concise, and free of typographical errors. Plan includes sound strategy for transition into the contract that ensures continuity of operations for the MCNOSC.	Plan contains less than 2% of typographical errors. All operational areas covered in plan.
Technical Status Meetings	C.4.1	A005	Minutes are clear, concise, and free of typographical errors. Agenda provided.	Minutes contain less than 2% of typographical errors. Agenda is clear.

Project Management Plan - Final	C.4.1	A006	Plan is clear, concise, and free of typographical errors. Plan covers all elements required in the SSCPAC PM Guide and provides meaningful guidance for schedule, scope, communication, and budget management.	Plan contains less than 2% of typographical errors. All elements from PM Guide covered.
Monthly Status Report (Cost, Schedule, Accomplishments)	C.4.1	A007	Reports are clear, concise, and free of typographical errors.	Monthly reports contain less than 2% of typographical errors. Monthly reports documents 80% or more of the monthly activities.
Meeting Minutes	C.4.1	A008	Minutes are clear, concise, and free of typographical errors.	Minutes contain less than 2% of typographical errors and contain 80% of meeting discussion items, as well as 100% of all follow-on actions.
Trip Report(s)	C.4.1	A009	Reports are clear, concise, and free of typographical errors.	Reports contain less than 2% of typographical errors. Reports document 80% or more of travel activities and 100% of action items and lessons learned.
EDM Weekly Status Report	C.4.3.2	A00A	Reports are clear, concise, and free of typographical errors.	Reports contain less than 2% of typographical errors. Reports document 80% or more of the weekly activities.

EDM SAN Capacity and Performance Report	C.4.3.2	A00B	Reports are clear, concise, and free of typographical errors.	Reports contain less than 2% of typographical errors. Reports include sufficient metrics to allow for performance measurement of the SAN capacity.
Design Documentation, Instructions and Proceedures	C.4.4	A00C	Reports are clear, concise, and free of typographical errors.	Reports contain less than 2% of typographical errors. Documentation includes design, instructions, and proceedures sufficient to enable a third party to understand and operate the task described.
Technical Findings Architecture Report	C.4.3.2	A00D	Reports are clear, concise, and free of typographical errors.	Reports contain less than 2% of typographical errors. Documentation includes all elements described in the PWS.
Tier III INS Status Report	C.4.3.3	A00E	Reports are clear, concise, and free of typographical errors. Reports include accurate log of Tier III INS events.	Reports contain less than 2% of typographical errors and capture all Tier III events and critical status information.
UC Status Report	C.4.3.3	A00F	Reports are clear, concise, and free of typographical errors. Format detailed in UC SOPs. Reports shall document UC incidents and meeting outcomes.	Reports contain less than 2% of typographical errors and contain 100% of incidents, 80% of meeting outcomes, and 100% of action items.

UC Network Architecture Report	C.4.3.3	A00G	Reports are clear, concise, and free of typographical errors.	Reports contain less than 2% of typographical errors. Reports contain UC Network Architecture Reviews of configurations and settings, delivered in format detailed in UC SOPs. Reports shall include identified security vulnerabilities, security incidents and conduct appropriate actions to report identified issues and recommend corrective action to the UC Government TPOC.
Watch Team Status Report	C.4.3.1	A00H	Reports are clear, concise, and free of typographical errors.	Reports contain less than 2% of typographical errors. Reports include work performed in previous week and work to be accomplished in the upcoming week.
Post-Incident Report	C.4.3.1	A00J	Reports are clear, concise, and free of typographical errors.	Reports contain less than 2% of typographical errors. Reports include reason for the outage, corrective actions taken, and any follow-on actions upon resolution of a trouble ticket for outage of service.
Service Desk Performance Metrics	C.4.3.1	A00K	Reports are clear, concise, and free of typographical errors.	Reports contain less than 2% of typographical errors. Generate, post, and retain historical information for weekly and monthly Service Desk performance measurements and

				include in reports.
IAVA Compliance Report	C.4.4.1	A00L	Reports are clear, concise, and free of typographical errors.	Perform information assurance scans utilizing Retina or ACAS to check for IAVA compliance.
ACAS Support Documentation	C.4.2.2	A00M	Documentation is clear, concise, and free of typographical errors.	Documentation contains less than 2% of typographical errors, as well as all elements required for IAVA compliance. See section C.5.2.2 for sub-elements that must be included.
Communications Weekly Status Reports	C.4.4	A00N	Reports are clear, concise, and free of typographical errors.	Reports contain less than 2% of typographical errors. Reports include incidents, trends, and other technical issues related to desktop support.
Critical (Priority 1) Incident, Service Request, and Work Order Resolution			Critical (Priority 1) incidents, service requests, and work orders must be resolved or completed within 8 hours. Records associated with priority 1 activities must be assigned to a technician within 10 minutes and updated every 90 minutes until resolution or completion. Resolution targets exclude times when the record is in the pending status.	90% of critical Priority incidents, service requests, and work orders are within target metrics.

High (Priority 2) Incident, Service Request, and Work Order Resolution			High (Priority 2) incidents, service requests, and work orders must be resolved or completed within 24 hours. Records associated with priority 2 activities must be assigned to a technician within 30 minutes and updated every 12 hours until resolution or completion. Resolution targets exclude times when the record is in the pending status. Tickets in pending status must be updated every 24 hours.	90% of high priority incidents, service requests, and work orders are within target metrics.
Medium (Priority 3) Incident, Service Request, and Work Order Resolution			Medium (Priority 3) incidents, service requests, and work orders must be resolved or completed within 5 business days. Records associated with priority 2 activities must be assigned to a technician within 60 minutes during business times and updated every 72 hours until resolution or completion. Resolution targets exclude times when the record is in the pending status. Tickets in pending status must be updated every 7 business days.	90% of medium priority incidents, service requests, and work orders are within target metrics.

Low (Priority 4) Incident, Service Request, and Work Order Resolution			Low (Priority 4) incidents, service requests, and work orders must be resolved or completed within 10 business days. Records associated with priority 2 activities must be assigned to a technician within 60 minutes during business times and updated every 7 days until resolution or completion. Resolution targets exclude times when the record is in the pending status. Tickets in pending status must be updated every 10 business days.	90% of low priority incidents, service requests, and work orders are within target metrics.